ARTICLE 5	**ARTICLE 4**
MINNESOTA CONSUMER DATA PRIVACY ACT	**CONSUMER DATA PRIVACY**

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

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

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

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

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

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

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

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

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

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

(1) a digital or physical photograph;

(2) an audio or video recording; or

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

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

(f) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of

57.4 personal data relating to the consumer. Acceptance of a general or broad terms of use or	20.24 personal data relating to the consumer. Acceptance of a general or broad terms of use or
57.5 similar document that contains descriptions of personal data processing along with other,	20.25 similar document that contains descriptions of personal data processing along with other,
57.6 unrelated information does not constitute consent. Hovering over, muting, pausing, or closing	20.26 unrelated information does not constitute consent. Hovering over, muting, pausing, or closing
57.7 a given piece of content does not constitute consent. A consent is not valid when the	20.27 a given piece of content does not constitute consent. A consent is not valid when the
57.8 consumer's indication has been obtained by a dark pattern. A consumer may revoke consent	20.28 consumer's indication has been obtained by a dark pattern. A consumer may revoke consent
57.9 previously given, consistent with this chapter.	20.29 previously given, consistent with this chapter.
57.10 (g) "Consumer" means a natural person who is a Minnesota resident acting only in an	20.30 (g) "Consumer" means a natural person who is a Minnesota resident acting only in an
57.11 individual or household context. Consumer does not include a natural person acting in a	20.31 individual or household context. Consumer does not include a natural person acting in a
57.12 commercial or employment context.	20.32 commercial or employment context.
57.13 (h) "Controller" means the natural or legal person which, alone or jointly with others,	21.1 (h) "Controller" means the natural or legal person who, alone or jointly with others,
57.14 determines the purposes and means of the processing of personal data.	21.2 determines the purposes and means of the processing of personal data.
57.15 (i) "Decisions that produce legal or similarly significant effects concerning the consumer"	21.3 (i) "Decisions that produce legal or similarly significant effects concerning the consumer"
57.16 means decisions made by the controller that result in the provision or denial by the controller	21.4 means decisions made by the controller that result in the provision or denial by the controller
57.17 of financial or lending services, housing, insurance, education enrollment or opportunity,	21.5 of financial or lending services, housing, insurance, education enrollment or opportunity,
57.18 criminal justice, employment opportunities, health care services, or access to essential goods	21.6 criminal justice, employment opportunities, health care services, or access to essential goods
57.19 or services.	21.7 or services.
57.20 (j) "Dark pattern" means a user interface designed or manipulated with the substantial	21.8 (j) "Dark pattern" means a user interface designed or manipulated with the substantial
57.21 effect of subverting or impairing user autonomy, decision making, or choice.	21.9 effect of subverting or impairing user autonomy, decision making, or choice.
57.22 (k) "Deidentified data" means data that cannot reasonably be used to infer information	21.10 (k) "Deidentified data" means data that cannot reasonably be used to infer information
57.23 about or otherwise be linked to an identified or identifiable natural person or a device linked	21.11 about or otherwise be linked to an identified or identifiable natural person or a device linked
57.24 to an identified or identifiable natural person, provided that the controller that possesses the	21.12 to an identified or identifiable natural person, provided that the controller that possesses the
57.25 data:	21.13 data:
57.26 (1) takes reasonable measures to ensure that the data cannot be associated with a natural	21.14 (1) takes reasonable measures to ensure that the data cannot be associated with a natural
57.27 person;	21.15 person;
57.28 (2) publicly commits to process the data only in a deidentified fashion and not attempt	21.16 (2) publicly commits to process the data only in a deidentified fashion and not attempt
57.29 to reidentify the data; and	21.17 to reidentify the data; and
57.30 (3) contractually obligates any recipients of the information to comply with all provisions	21.18 (3) contractually obligates any recipients of the information to comply with all provisions
57.31 of this paragraph.	21.19 of this paragraph.
58.1 (l) "Delete" means to remove or destroy information so that it is not maintained in human-	21.20 (l) "Delete" means to remove or destroy information so that it is not maintained in human-
58.2 or machine-readable form and cannot be retrieved or utilized in the ordinary course of	21.21 or machine-readable form and cannot be retrieved or utilized in the ordinary course of
58.3 business.	21.22 business.
58.4 (m) "Genetic information" has the meaning given in section 13.386, subdivision 1.	21.23 (m) "Genetic information" has the meaning given in section 13.386, subdivision 1.
58.5 (n) "Identified or identifiable natural person" means a person who can be readily	21.24 (n) "Identified or identifiable natural person" means a person who can be readily
58.6 identified, directly or indirectly.	21.25 identified, directly or indirectly.

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

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

58.15 (q) "Process" or "processing" means any operation or set of operations that are performed
58.16 on personal data or on sets of personal data, whether or not by automated means, including
58.17 but not limited to the collection, use, storage, disclosure, analysis, deletion, or modification
58.18 of personal data.

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

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

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

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

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

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

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

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

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

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

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

22.3 (q) "Process" or "processing" means any operation or set of operations that are performed
22.4 on personal data or on sets of personal data, whether or not by automated means, including
22.5 but not limited to the collection, use, storage, disclosure, analysis, deletion, or modification
22.6 of personal data.

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

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

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

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

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

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

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

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

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

59.9 (6) the exchange of personal data between the producer of a good or service and	22.30 (6) the exchange of personal data between the producer of a good or service and
59.10 authorized agents of the producer who sell and service the goods and services, to enable	22.31 authorized agents of the producer who sell and service the goods and services, to enable
59.11 the cooperative provisioning of goods and services by both the producer and the producer's	23.1 the cooperative provisioning of goods and services by both the producer and the producer's
59.12 agents.	23.2 agents.
59.13 (v) Sensitive data is a form of personal data. "Sensitive data" means:	23.3 (v) Sensitive data is a form of personal data. "Sensitive data" means:
59.14 (1) personal data revealing racial or ethnic origin, religious beliefs, mental or physical	23.4 (1) personal data revealing racial or ethnic origin, religious beliefs, mental or physical
59.15 health condition or diagnosis, sexual orientation, or citizenship or immigration status;	23.5 health condition or diagnosis, sexual orientation, or citizenship or immigration status;
59.16 (2) the processing of biometric data or genetic information for the purpose of uniquely	23.6 (2) the processing of biometric data or genetic information for the purpose of uniquely
59.17 identifying an individual;	23.7 identifying an individual;
59.18 (3) the personal data of a known child; or	23.8 (3) the personal data of a known child; or
59.19 (4) specific geolocation data.	23.9 (4) specific geolocation data.
59.20 (w) "Specific geolocation data" means information derived from technology, including	23.10 (w) "Specific geolocation data" means information derived from technology, including
59.21 but not limited to global positioning system level latitude and longitude coordinates or other	23.11 but not limited to global positioning system level latitude and longitude coordinates or other
59.22 mechanisms, that directly identifies the geographic coordinates of a consumer or a device	23.12 mechanisms, that directly identifies the geographic coordinates of a consumer or a device
59.23 linked to a consumer with an accuracy of more than three decimal degrees of latitude and	23.13 linked to a consumer with an accuracy of more than three decimal degrees of latitude and
59.24 longitude or the equivalent in an alternative geographic coordinate system, or a street address	23.14 longitude or the equivalent in an alternative geographic coordinate system, or a street address
59.25 derived from the coordinates. Specific geolocation data does not include the content of	23.15 derived from the coordinates. Specific geolocation data does not include the content of
59.26 communications, the contents of databases containing street address information which are	23.16 communications, the contents of databases containing street address information which are
59.27 accessible to the public as authorized by law, or any data generated by or connected to	23.17 accessible to the public as authorized by law, or any data generated by or connected to
59.28 advanced utility metering infrastructure systems or other equipment for use by a public	23.18 advanced utility metering infrastructure systems or other equipment for use by a public
59.29 utility.	23.19 utility.
59.30 (x) "Targeted advertising" means displaying advertisements to a consumer where the	23.20 (x) "Targeted advertising" means displaying advertisements to a consumer where the
59.31 advertisement is selected based on personal data obtained or inferred from the consumer's	23.21 advertisement is selected based on personal data obtained or inferred from the consumer's
60.1 activities over time and across nonaffiliated websites or online applications to predict the	23.22 activities over time and across nonaffiliated websites or online applications to predict the
60.2 consumer's preferences or interests. Targeted advertising does not include:	23.23 consumer's preferences or interests. Targeted advertising does not include:
60.3 (1) advertising based on activities within a controller's own websites or online	23.24 (1) advertising based on activities within a controller's own websites or online
60.4 applications;	23.25 applications;
60.5 (2) advertising based on the context of a consumer's current search query or visit to a	23.26 (2) advertising based on the context of a consumer's current search query or visit to a
60.6 website or online application;	23.27 website or online application;
60.7 (3) advertising to a consumer in response to the consumer's request for information or	23.28 (3) advertising to a consumer in response to the consumer's request for information or
60.8 feedback; or	23.29 feedback; or
60.9 (4) processing personal data solely for measuring or reporting advertising performance,	23.30 (4) processing personal data solely for measuring or reporting advertising performance,
60.10 reach, or frequency.	23.31 reach, or frequency.
60.11 (y) "Third party" means a natural or legal person, public authority, agency, or body other	24.1 (y) "Third party" means a natural or legal person, public authority, agency, or body other
60.12 than the consumer, controller, processor, or an affiliate of the processor or the controller.	24.2 than the consumer, controller, processor, or an affiliate of the processor or the controller.

60.13 (z) "Trade secret" has the meaning given in section 325C.01, subdivision 5.	24.3 (z) "Trade secret" has the meaning given in section 325C.01, subdivision 5.
60.14 Sec. 4. **[325O.03] SCOPE; EXCLUSIONS.**	24.4 Sec. 4. **[325O.03] SCOPE; EXCLUSIONS.**
60.15 Subdivision 1. **Scope.** (a) This chapter applies to legal entities that conduct business in 60.16 Minnesota or produce products or services that are targeted to residents of Minnesota, and 60.17 that satisfy one or more of the following thresholds:	24.5 Subdivision 1. **Scope.** (a) This chapter applies to legal entities that conduct business in 24.6 Minnesota or produce products or services that are targeted to residents of Minnesota, and 24.7 that satisfy one or more of the following thresholds:
60.18 (1) during a calendar year, controls or processes personal data of 100,000 consumers or 60.19 more, excluding personal data controlled or processed solely for the purpose of completing 60.20 a payment transaction; or	24.8 (1) during a calendar year, controls or processes personal data of 100,000 consumers or 24.9 more, excluding personal data controlled or processed solely for the purpose of completing 24.10 a payment transaction; or
60.21 (2) derives over 25 percent of gross revenue from the sale of personal data and processes 60.22 or controls personal data of 25,000 consumers or more.	24.11 (2) derives over 25 percent of gross revenue from the sale of personal data and processes 24.12 or controls personal data of 25,000 consumers or more.
60.23 (b) A controller or processor acting as a technology provider under section 13.32 shall 60.24 comply with this chapter and section 13.32, except that when the provisions of section 13.32 60.25 conflict with this chapter, section 13.32 prevails.	24.13 (b) A controller or processor acting as a technology provider under section 13.32 shall 24.14 comply with this chapter and section 13.32, except that when the provisions of section 13.32 24.15 conflict with this chapter, section 13.32 prevails.
60.26 Subd. 2. **Exclusions.** (a) This chapter does not apply to the following entities, activities, 60.27 or types of information:	24.16 Subd. 2. **Exclusions.** (a) This chapter does not apply to the following entities, activities, 24.17 or types of information:
60.28 (1) a government entity, as defined by section 13.02, subdivision 7a;	24.18 (1) a government entity, as defined by section 13.02, subdivision 7a;
60.29 (2) a federally recognized Indian tribe;	24.19 (2) a federally recognized Indian tribe;
60.30 (3) information that meets the definition of:	24.20 (3) information that meets the definition of:
61.1 (i) protected health information, as defined by and for purposes of the Health Insurance 61.2 Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;	24.21 (i) protected health information, as defined by and for purposes of the Health Insurance 24.22 Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;
61.3 (ii) health records, as defined in section 144.291, subdivision 2;	24.23 (ii) health records, as defined in section 144.291, subdivision 2;
61.4 (iii) patient identifying information for purposes of Code of Federal Regulations, title 61.5 42, part 2, established pursuant to United States Code, title 42, section 290dd-2;	24.24 (iii) patient identifying information for purposes of Code of Federal Regulations, title 24.25 42, part 2, established pursuant to United States Code, title 42, section 290dd-2;
61.6 (iv) identifiable private information for purposes of the federal policy for the protection 61.7 of human subjects, Code of Federal Regulations, title 45, part 46; identifiable private 61.8 information that is otherwise information collected as part of human subjects research 61.9 pursuant to the good clinical practice guidelines issued by the International Council for 61.10 Harmonisation; the protection of human subjects under Code of Federal Regulations, title 61.11 21, parts 50 and 56; or personal data used or shared in research conducted in accordance 61.12 with one or more of the requirements set forth in this paragraph;	24.26 (iv) identifiable private information for purposes of the federal policy for the protection 24.27 of human subjects, Code of Federal Regulations, title 45, part 46; identifiable private 24.28 information that is otherwise information collected as part of human subjects research 24.29 pursuant to the good clinical practice guidelines issued by the International Council for 24.30 Harmonisation; the protection of human subjects under Code of Federal Regulations, title 25.1 21, parts 50 and 56; or personal data used or shared in research conducted in accordance 25.2 with one or more of the requirements set forth in this paragraph;
61.13 (v) information and documents created for purposes of the federal Health Care Quality 61.14 Improvement Act of 1986, Public Law 99-660, and related regulations; or	25.3 (v) information and documents created for purposes of the federal Health Care Quality 25.4 Improvement Act of 1986, Public Law 99-660, and related regulations; or
61.15 (vi) patient safety work product for purposes of Code of Federal Regulations, title 42, 61.16 part 3, established pursuant to United States Code, title 42, sections 299b-21 to 299b-26;	25.5 (vi) patient safety work product for purposes of Code of Federal Regulations, title 42, 25.6 part 3, established pursuant to United States Code, title 42, sections 299b-21 to 299b-26;

61.17 (4) information that is derived from any of the health care-related information listed in 61.18 clause (3), but that has been deidentified in accordance with the requirements for 61.19 deidentification set forth in Code of Federal Regulations, title 45, part 164;	25.7 (4) information that is derived from any of the health care-related information listed in 25.8 clause (3), but that has been deidentified in accordance with the requirements for 25.9 deidentification set forth in Code of Federal Regulations, title 45, part 164;

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

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

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

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

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

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

61.25   (iii) a program or a qualified service organization, as defined by Code of Federal
61.26 Regulations, title 42, part 2, established pursuant to United States Code, title 42, section
61.27 290dd-2;

25.15   (iii) a program or a qualified service organization, as defined by Code of Federal
25.16 Regulations, title 42, part 2, established pursuant to United States Code, title 42, section
25.17 290dd-2;

61.28   (6) information that is:

25.18   (6) information that is:

61.29   (i) maintained by an entity that meets the definition of health care provider under Code
61.30 of Federal Regulations, title 45, section 160.103, to the extent that the entity maintains the
61.31 information in the manner required of covered entities with respect to protected health
62.1 information for purposes of the Health Insurance Portability and Accountability Act of
62.2 1996, Public Law 104-191, and related regulations;

25.19   (i) maintained by an entity that meets the definition of health care provider under Code
25.20 of Federal Regulations, title 45, section 160.103, to the extent that the entity maintains the
25.21 information in the manner required of covered entities with respect to protected health
25.22 information for purposes of the Health Insurance Portability and Accountability Act of
25.23 1996, Public Law 104-191, and related regulations;

62.3   (ii) included in a limited data set, as described under Code of Federal Regulations, title
62.4 45, part 164.514(e), to the extent that the information is used, disclosed, and maintained in
62.5 the manner specified by that part;

25.24   (ii) included in a limited data set, as described under Code of Federal Regulations, title
25.25 45, part 164.514(e), to the extent that the information is used, disclosed, and maintained in
25.26 the manner specified by that part;

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

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

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

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

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

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

62.15   (8) an activity involving the collection, maintenance, disclosure, sale, communication,
62.16 or use of any personal data bearing on a consumer's credit worthiness, credit standing, credit
62.17 capacity, character, general reputation, personal characteristics, or mode of living by a
62.18 consumer reporting agency, as defined in United States Code, title 15, section 1681a(f), by
62.19 a furnisher of information, as set forth in United States Code, title 15, section 1681s-2, who
62.20 provides information for use in a consumer report, as defined in United States Code, title
62.21 15, section 1681a(d), and by a user of a consumer report, as set forth in United States Code,
62.22 title 15, section 1681b, except that information is only excluded under this paragraph to the

26.5   (8) an activity involving the collection, maintenance, disclosure, sale, communication,
26.6 or use of any personal data bearing on a consumer's credit worthiness, credit standing, credit
26.7 capacity, character, general reputation, personal characteristics, or mode of living by a
26.8 consumer reporting agency, as defined in United States Code, title 15, section 1681a(f), by
26.9 a furnisher of information, as set forth in United States Code, title 15, section 1681s-2, who
26.10 provides information for use in a consumer report, as defined in United States Code, title
26.11 15, section 1681a(d), and by a user of a consumer report, as set forth in United States Code,
26.12 title 15, section 1681b, except that information is only excluded under this paragraph to the

62.23 extent that the activity involving the collection, maintenance, disclosure, sale, communication,	26.13 extent that the activity involving the collection, maintenance, disclosure, sale, communication,
62.24 or use of the information by the agency, furnisher, or user is subject to regulation under the	26.14 or use of the information by the agency, furnisher, or user is subject to regulation under the
62.25 federal Fair Credit Reporting Act, United States Code, title 15, sections 1681 to 1681x, and	26.15 federal Fair Credit Reporting Act, United States Code, title 15, sections 1681 to 1681x, and
62.26 the information is not collected, maintained, used, communicated, disclosed, or sold except	26.16 the information is not collected, maintained, used, communicated, disclosed, or sold except
62.27 as authorized by the Fair Credit Reporting Act;	26.17 as authorized by the Fair Credit Reporting Act;
62.28 (9) personal data collected, processed, sold, or disclosed pursuant to the federal	26.18 (9) personal data collected, processed, sold, or disclosed pursuant to the federal
62.29 Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations, if the	26.19 Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations, if the
62.30 collection, processing, sale, or disclosure is in compliance with that law;	26.20 collection, processing, sale, or disclosure is in compliance with that law;
62.31 (10) personal data collected, processed, sold, or disclosed pursuant to the federal Driver's	26.21 (10) personal data collected, processed, sold, or disclosed pursuant to the federal Driver's
62.32 Privacy Protection Act of 1994, United States Code, title 18, sections 2721 to 2725, if the	26.22 Privacy Protection Act of 1994, United States Code, title 18, sections 2721 to 2725, if the
62.33 collection, processing, sale, or disclosure is in compliance with that law;	26.23 collection, processing, sale, or disclosure is in compliance with that law;
63.1 (11) personal data regulated by the federal Family Educational Rights and Privacy Act,	26.24 (11) personal data regulated by the federal Family Educational Rights and Privacy Act,
63.2 United States Code, title 20, section 1232g, and implementing regulations;	26.25 United States Code, title 20, section 1232g, and implementing regulations;
63.3 (12) personal data collected, processed, sold, or disclosed pursuant to the federal Farm	26.26 (12) personal data collected, processed, sold, or disclosed pursuant to the federal Farm
63.4 Credit Act of 1971, as amended, United States Code, title 12, sections 2001 to 2279cc, and	26.27 Credit Act of 1971, as amended, United States Code, title 12, sections 2001 to 2279cc, and
63.5 implementing regulations, Code of Federal Regulations, title 12, part 600, if the collection,	26.28 implementing regulations, Code of Federal Regulations, title 12, part 600, if the collection,
63.6 processing, sale, or disclosure is in compliance with that law;	26.29 processing, sale, or disclosure is in compliance with that law;
63.7 (13) data collected or maintained:	26.30 (13) data collected or maintained:
63.8 (i) in the course of an individual acting as a job applicant to or an employee, owner,	26.31 (i) in the course of an individual acting as a job applicant to or an employee, owner,
63.9 director, officer, medical staff member, or contractor of a business if the data is collected	26.32 director, officer, medical staff member, or contractor of a business if the data is collected
63.10 and used solely within the context of the role;	26.33 and used solely within the context of the role;
63.11 (ii) as the emergency contact information of an individual under item (i) if used solely	27.1 (ii) as the emergency contact information of an individual under item (i) if used solely
63.12 for emergency contact purposes; or	27.2 for emergency contact purposes; or
63.13 (iii) that is necessary for the business to retain to administer benefits for another individual	27.3 (iii) that is necessary for the business to retain to administer benefits for another individual
63.14 relating to the individual under item (i) if used solely for the purposes of administering those	27.4 relating to the individual under item (i) if used solely for the purposes of administering those
63.15 benefits;	27.5 benefits;
63.16 (14) personal data collected, processed, sold, or disclosed pursuant to the Minnesota	27.6 (14) personal data collected, processed, sold, or disclosed pursuant to the Minnesota
63.17 Insurance Fair Information Reporting Act in sections 72A.49 to 72A.505;	27.7 Insurance Fair Information Reporting Act in sections 72A.49 to 72A.505;
63.18 (15) data collected, processed, sold, or disclosed as part of a payment-only credit, check,	27.8 (15) data collected, processed, sold, or disclosed as part of a payment-only credit, check,
63.19 or cash transaction where no data about consumers, as defined in section 325O.02, are	27.9 or cash transaction where no data about consumers, as defined in section 325O.02, are
63.20 retained;	27.10 retained;
63.21 (16) a state or federally chartered bank or credit union, or an affiliate or subsidiary that	27.11 (16) a state or federally chartered bank or credit union, or an affiliate or subsidiary that
63.22 is principally engaged in financial activities, as described in United States Code, title 12,	27.12 is principally engaged in financial activities, as described in United States Code, title 12,
63.23 section 1843(k);	27.13 section 1843(k);
63.24 (17) information that originates from, or is intermingled so as to be indistinguishable	27.14 (17) information that originates from, or is intermingled so as to be indistinguishable
63.25 from, information described in clause (8) and that a person licensed under chapter 56 collects,	27.15 from, information described in clause (8) and that a person licensed under chapter 56 collects,

63.26 processes, uses, or maintains in the same manner as is required under the laws and regulations
63.27 specified in clause (8);

63.28   (18) an insurance company, as defined in section 60A.02, subdivision 4, an insurance
63.29 producer, as defined in section 60K.31, subdivision 6, a third-party administrator of
63.30 self-insurance, or an affiliate or subsidiary of any entity identified in this clause that is
63.31 principally engaged in financial activities, as described in United States Code, title 12,
63.32 section 1843(k), except that this clause does not apply to a person that, alone or in
64.1 combination with another person, establishes and maintains a self-insurance program that
64.2 does not otherwise engage in the business of entering into policies of insurance;

64.3   (19) a small business, as defined by the United States Small Business Administration
64.4 under Code of Federal Regulations, title 13, part 121, except that a small business identified
64.5 in this clause is subject to section 325O.075;

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

64.8   (21) an air carrier subject to the federal Airline Deregulation Act, Public Law 95-504,
64.9 only to the extent that an air carrier collects personal data related to prices, routes, or services
64.10 and only to the extent that the provisions of the Airline Deregulation Act preempt the
64.11 requirements of this chapter.

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

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

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

64.18   (b) Processors are responsible under this chapter for adhering to the instructions of the
64.19 controller and assisting the controller to meet the controller's obligations under this chapter.
64.20 Assistance under this paragraph shall include the following:

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

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

27.16 processes, uses, or maintains in the same manner as is required under the laws and regulations
27.17 specified in clause (8);

27.18   (18) an insurance company, as defined in section 60A.02, subdivision 4, an insurance
27.19 producer, as defined in section 60K.31, subdivision 6, a third-party administrator of
27.20 self-insurance, or an affiliate or subsidiary of any entity identified in this clause that is
27.21 principally engaged in financial activities, as described in United States Code, title 12,
27.22 section 1843(k), except that this clause does not apply to a person that, alone or in
27.23 combination with another person, establishes and maintains a self-insurance program that
27.24 does not otherwise engage in the business of entering into policies of insurance;

27.25   (19) a small business, as defined by the United States Small Business Administration
27.26 under Code of Federal Regulations, title 13, part 121, except that a small business identified
27.27 in this clause is subject to section 325O.075;

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

27.30   (21) an air carrier subject to the federal Airline Deregulation Act, Public Law 95-504,
27.31 only to the extent that an air carrier collects personal data related to prices, routes, or services
27.32 and only to the extent that the provisions of the Airline Deregulation Act preempt the
27.33 requirements of this chapter.

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

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

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

28.7   (b) Processors are responsible under this chapter for adhering to the instructions of the
28.8 controller and assisting the controller to meet the controller's obligations under this chapter.
28.9 Assistance under this paragraph shall include the following:

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

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

64.31 (c) A contract between a controller and a processor shall govern the processor's data	28.20 (c) A contract between a controller and a processor shall govern the processor's data
64.32 processing procedures with respect to processing performed on behalf of the controller. The	28.21 processing procedures with respect to processing performed on behalf of the controller. The
65.1 contract shall be binding and clearly set forth instructions for processing data, the nature	28.22 contract shall be binding and clearly set forth instructions for processing data, the nature
65.2 and purpose of processing, the type of data subject to processing, the duration of processing,	28.23 and purpose of processing, the type of data subject to processing, the duration of processing,
65.3 and the rights and obligations of both parties. The contract shall also require that the	28.24 and the rights and obligations of both parties. The contract shall also require that the
65.4 processor:	28.25 processor:
65.5 (1) ensure that each person processing the personal data is subject to a duty of	28.26 (1) ensure that each person processing the personal data is subject to a duty of
65.6 confidentiality with respect to the data; and	28.27 confidentiality with respect to the data; and
65.7 (2) engage a subcontractor only (i) after providing the controller with an opportunity to	28.28 (2) engage a subcontractor only (i) after providing the controller with an opportunity to
65.8 object, and (ii) pursuant to a written contract in accordance with paragraph (e) that requires	28.29 object, and (ii) pursuant to a written contract in accordance with paragraph (e) that requires
65.9 the subcontractor to meet the obligations of the processor with respect to the personal data.	28.30 the subcontractor to meet the obligations of the processor with respect to the personal data.
65.10 (d) Taking into account the context of processing, the controller and the processor shall	28.31 (d) Taking into account the context of processing, the controller and the processor shall
65.11 implement appropriate technical and organizational measures to ensure a level of security	28.32 implement appropriate technical and organizational measures to ensure a level of security
65.12 appropriate to the risk and establish a clear allocation of the responsibilities between the	29.1 appropriate to the risk and establish a clear allocation of the responsibilities between the
65.13 controller and the processor to implement the technical and organizational measures.	29.2 controller and the processor to implement the technical and organizational measures.
65.14 (e) Processing by a processor shall be governed by a contract between the controller and	29.3 (e) Processing by a processor shall be governed by a contract between the controller and
65.15 the processor that is binding on both parties and that sets out the processing instructions to	29.4 the processor that is binding on both parties and that sets out the processing instructions to
65.16 which the processor is bound, including the nature and purpose of the processing, the type	29.5 which the processor is bound, including the nature and purpose of the processing, the type
65.17 of personal data subject to the processing, the duration of the processing, and the obligations	29.6 of personal data subject to the processing, the duration of the processing, and the obligations
65.18 and rights of both parties. The contract shall include the requirements imposed by this	29.7 and rights of both parties. The contract shall include the requirements imposed by this
65.19 paragraph, paragraphs (c) and (d), as well as the following requirements:	29.8 paragraph, paragraphs (c) and (d), as well as the following requirements:
65.20 (1) at the choice of the controller, the processor shall delete or return all personal data	29.9 (1) at the choice of the controller, the processor shall delete or return all personal data
65.21 to the controller as requested at the end of the provision of services, unless retention of the	29.10 to the controller as requested at the end of the provision of services, unless retention of the
65.22 personal data is required by law;	29.11 personal data is required by law;
65.23 (2) upon a reasonable request from the controller, the processor shall make available to	29.12 (2) upon a reasonable request from the controller, the processor shall make available to
65.24 the controller all information necessary to demonstrate compliance with the obligations in	29.13 the controller all information necessary to demonstrate compliance with the obligations in
65.25 this chapter; and	29.14 this chapter; and
65.26 (3) the processor shall allow for, and contribute to, reasonable assessments and inspections	29.15 (3) the processor shall allow for, and contribute to, reasonable assessments and inspections
65.27 by the controller or the controller's designated assessor. Alternatively, the processor may	29.16 by the controller or the controller's designated assessor. Alternatively, the processor may
65.28 arrange for a qualified and independent assessor to conduct, at least annually and at the	29.17 arrange for a qualified and independent assessor to conduct, at least annually and at the
65.29 processor's expense, an assessment of the processor's policies and technical and organizational	29.18 processor's expense, an assessment of the processor's policies and technical and organizational
65.30 measures in support of the obligations under this chapter. The assessor must use an	29.19 measures in support of the obligations under this chapter. The assessor must use an
65.31 appropriate and accepted control standard or framework and assessment procedure for	29.20 appropriate and accepted control standard or framework and assessment procedure for
65.32 assessments as applicable, and shall provide a report of an assessment to the controller upon	29.21 assessments as applicable, and shall provide a report of an assessment to the controller upon
65.33 request.	29.22 request.
66.1 (f) In no event shall any contract relieve a controller or a processor from the liabilities	29.23 (f) In no event shall any contract relieve a controller or a processor from the liabilities
66.2 imposed on a controller or processor by virtue of the controller's or processor's roles in the	29.24 imposed on a controller or processor by virtue of the controller's or processor's roles in the
66.3 processing relationship under this chapter.	29.25 processing relationship under this chapter.

66.4 (g) Determining whether a person is acting as a controller or processor with respect to	29.26 (g) Determining whether a person is acting as a controller or processor with respect to
66.5 a specific processing of data is a fact-based determination that depends upon the context in	29.27 a specific processing of data is a fact-based determination that depends upon the context in
66.6 which personal data are to be processed. A person that is not limited in the person's processing	29.28 which personal data are to be processed. A person that is not limited in the person's processing
66.7 of personal data pursuant to a controller's instructions, or that fails to adhere to a controller's	29.29 of personal data pursuant to a controller's instructions, or that fails to adhere to a controller's
66.8 instructions, is a controller and not a processor with respect to a specific processing of data.	29.30 instructions, is a controller and not a processor with respect to a specific processing of data.
66.9 A processor that continues to adhere to a controller's instructions with respect to a specific	29.31 A processor that continues to adhere to a controller's instructions with respect to a specific
66.10 processing of personal data remains a processor. If a processor begins, alone or jointly with	29.32 processing of personal data remains a processor. If a processor begins, alone or jointly with
66.11 others, determining the purposes and means of the processing of personal data, the processor	29.33 others, determining the purposes and means of the processing of personal data, the processor
66.12 is a controller with respect to the processing.	29.34 is a controller with respect to the processing.
66.13 Sec. 6. **[325O.05] CONSUMER PERSONAL DATA RIGHTS.**	30.1 Sec. 6. **[325O.05] CONSUMER PERSONAL DATA RIGHTS.**
66.14 Subdivision 1. **Consumer rights provided.** (a) Except as provided in this chapter, a	30.2 Subdivision 1. **Consumer rights provided.** (a) Except as provided in this chapter, a
66.15 controller must comply with a request to exercise the consumer rights provided in this	30.3 controller must comply with a request to exercise the consumer rights provided in this
66.16 subdivision.	30.4 subdivision.
66.17 (b) A consumer has the right to confirm whether or not a controller is processing personal	30.5 (b) A consumer has the right to confirm whether or not a controller is processing personal
66.18 data concerning the consumer and access the categories of personal data the controller is	30.6 data concerning the consumer and access the categories of personal data the controller is
66.19 processing.	30.7 processing.
66.20 (c) A consumer has the right to correct inaccurate personal data concerning the consumer,	30.8 (c) A consumer has the right to correct inaccurate personal data concerning the consumer,
66.21 taking into account the nature of the personal data and the purposes of the processing of the	30.9 taking into account the nature of the personal data and the purposes of the processing of the
66.22 personal data.	30.10 personal data.
66.23 (d) A consumer has the right to delete personal data concerning the consumer.	30.11 (d) A consumer has the right to delete personal data concerning the consumer.
66.24 (e) A consumer has the right to obtain personal data concerning the consumer, which	30.12 (e) A consumer has the right to obtain personal data concerning the consumer, which
66.25 the consumer previously provided to the controller, in a portable and, to the extent technically	30.13 the consumer previously provided to the controller, in a portable and, to the extent technically
66.26 feasible, readily usable format that allows the consumer to transmit the data to another	30.14 feasible, readily usable format that allows the consumer to transmit the data to another
66.27 controller without hindrance, where the processing is carried out by automated means.	30.15 controller without hindrance, where the processing is carried out by automated means.
66.28 (f) A consumer has the right to opt out of the processing of personal data concerning	30.16 (f) A consumer has the right to opt out of the processing of personal data concerning
66.29 the consumer for purposes of targeted advertising, the sale of personal data, or profiling in	30.17 the consumer for purposes of targeted advertising, the sale of personal data, or profiling in
66.30 furtherance of automated decisions that produce legal effects concerning a consumer or	30.18 furtherance of automated decisions that produce legal effects concerning a consumer or
66.31 similarly significant effects concerning a consumer.	30.19 similarly significant effects concerning a consumer.
66.32 (g) If a consumer's personal data is profiled in furtherance of decisions that produce	30.20 (g) If a consumer's personal data is profiled in furtherance of decisions that produce
66.33 legal effects concerning a consumer or similarly significant effects concerning a consumer,	30.21 legal effects concerning a consumer or similarly significant effects concerning a consumer,
67.1 the consumer has the right to question the result of the profiling, to be informed of the reason	30.22 the consumer has the right to question the result of the profiling, to be informed of the reason
67.2 that the profiling resulted in the decision, and, if feasible, to be informed of what actions	30.23 that the profiling resulted in the decision, and, if feasible, to be informed of what actions
67.3 the consumer might have taken to secure a different decision and the actions that the	30.24 the consumer might have taken to secure a different decision and the actions that the
67.4 consumer might take to secure a different decision in the future. The consumer has the right	30.25 consumer might take to secure a different decision in the future. The consumer has the right
67.5 to review the consumer's personal data used in the profiling. If the decision is determined	30.26 to review the consumer's personal data used in the profiling. If the decision is determined
67.6 to have been based upon inaccurate personal data, taking into account the nature of the	30.27 to have been based upon inaccurate personal data, taking into account the nature of the
67.7 personal data and the purposes of the processing of the personal data, the consumer has the	30.28 personal data and the purposes of the processing of the personal data, the consumer has the

67.8 right to have the data corrected and the profiling decision reevaluated based upon the	30.29 right to have the data corrected and the profiling decision reevaluated based upon the
67.9 corrected data.	30.30 corrected data.

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

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

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

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

67.22   (d) A consumer may designate another person as the consumer's authorized agent to
67.23   exercise the consumer's right to opt out of the processing of the consumer's personal data
67.24   for purposes of targeted advertising and sale under subdivision 1, paragraph (f), on the
67.25   consumer's behalf. A consumer may designate an authorized agent by way of, among other
67.26   things, a technology, including but not limited to an Internet link or a browser setting,
67.27   browser extension, or global device setting, indicating the consumer's intent to opt out of
67.28   the processing. A controller shall comply with an opt-out request received from an authorized
67.29   agent if the controller is able to verify, with commercially reasonable effort, the identity of
67.30   the consumer and the authorized agent's authority to act on the consumer's behalf.

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

68.3   (1) not unfairly disadvantage another controller;

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

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

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

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

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

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

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

31.11   (d) A consumer may designate another person as the consumer's authorized agent to
31.12   exercise the consumer's right to opt out of the processing of the consumer's personal data
31.13   for purposes of targeted advertising and sale under subdivision 1, paragraph (f), on the
31.14   consumer's behalf. A consumer may designate an authorized agent by way of, among other
31.15   things, a technology, including but not limited to an Internet link or a browser setting,
31.16   browser extension, or global device setting, indicating the consumer's intent to opt out of
31.17   the processing. A controller shall comply with an opt-out request received from an authorized
31.18   agent if the controller is able to verify, with commercially reasonable effort, the identity of
31.19   the consumer and the authorized agent's authority to act on the consumer's behalf.

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

31.26   (1) not unfairly disadvantage another controller;

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

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

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

68.10 (5) enable the controller to accurately determine whether the consumer is a Minnesota	32.1 (5) enable the controller to accurately determine whether the consumer is a Minnesota
68.11 resident and whether the consumer has made a legitimate request to opt out of any sale of	32.2 resident and whether the consumer has made a legitimate request to opt out of any sale of
68.12 the consumer's personal data or targeted advertising. For purposes of this paragraph, the	32.3 the consumer's personal data or targeted advertising. For purposes of this paragraph, the
68.13 use of an Internet protocol address to estimate the consumer's location is sufficient to	32.4 use of an Internet protocol address to estimate the consumer's location is sufficient to
68.14 determine the consumer's residence.	32.5 determine the consumer's residence.

68.15   (b) If a consumer's opt-out request is exercised through the platform, technology, or
68.16 mechanism required under paragraph (a), and the request conflicts with the consumer's
68.17 existing controller-specific privacy setting or voluntary participation in a controller's bona
68.18 fide loyalty, rewards, premium features, discounts, or club card program, the controller
68.19 must comply with the consumer's opt-out preference signal but may also notify the consumer
68.20 of the conflict and provide the consumer a choice to confirm the controller-specific privacy
68.21 setting or participation in the controller's program.

32.6   (b) If a consumer's opt-out request is exercised through the platform, technology, or
32.7 mechanism required under paragraph (a), and the request conflicts with the consumer's
32.8 existing controller-specific privacy setting or voluntary participation in a controller's bona
32.9 fide loyalty, rewards, premium features, discounts, or club card program, the controller
32.10 must comply with the consumer's opt-out preference signal but may also notify the consumer
32.11 of the conflict and provide the consumer a choice to confirm the controller-specific privacy
32.12 setting or participation in the controller's program.

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

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

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

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

68.26   Subd. 4. **Controller response to consumer requests.** (a) Except as provided in this
68.27 chapter, a controller must comply with a request to exercise the rights pursuant to subdivision
68.28 1.

32.17   Subd. 4. **Controller response to consumer requests.** (a) Except as provided in this
32.18 chapter, a controller must comply with a request to exercise the rights pursuant to subdivision
32.19 1.

68.29   (b) A controller must provide one or more secure and reliable means for consumers to
68.30 submit a request to exercise the consumer rights under this section. The means made available
68.31 must take into account the ways in which consumers interact with the controller and the
68.32 need for secure and reliable communication of the requests.

32.20   (b) A controller must provide one or more secure and reliable means for consumers to
32.21 submit a request to exercise the consumer's rights under this section. The means made
32.22 available must take into account the ways in which consumers interact with the controller
32.23 and the need for secure and reliable communication of the requests.

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

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

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

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

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

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

69.12   (f) If a controller does not take action on a consumer's request, the controller must inform
69.13 the consumer without undue delay and at the latest within 45 days of receipt of the request

33.3   (f) If a controller does not take action on a consumer's request, the controller must inform
33.4 the consumer without undue delay and at the latest within 45 days of receipt of the request

69.14 of the reasons for not taking action and instructions for how to appeal the decision with the	33.5 of the reasons for not taking action and instructions for how to appeal the decision with the
69.15 controller as described in subdivision 3.	33.6 controller as described in subdivision 5.
69.16 (g) Information provided under this section must be provided by the controller free of	33.7 (g) Information provided under this section must be provided by the controller free of
69.17 charge, up to twice annually to the consumer. Where requests from a consumer are manifestly	33.8 charge up to twice annually to the consumer. Where requests from a consumer are manifestly
69.18 unfounded or excessive, in particular because of the repetitive character of the requests, the	33.9 unfounded or excessive, in particular because of the repetitive character of the requests, the
69.19 controller may either charge a reasonable fee to cover the administrative costs of complying	33.10 controller may either charge a reasonable fee to cover the administrative costs of complying
69.20 with the request, or refuse to act on the request. The controller bears the burden of	33.11 with the request, or refuse to act on the request. The controller bears the burden of
69.21 demonstrating the manifestly unfounded or excessive character of the request.	33.12 demonstrating the manifestly unfounded or excessive character of the request.
69.22 (h) A controller is not required to comply with a request to exercise any of the rights	33.13 (h) A controller is not required to comply with a request to exercise any of the rights
69.23 under subdivision 1, paragraphs (b) to (h), if the controller is unable to authenticate the	33.14 under subdivision 1, paragraphs (b) to (h), if the controller is unable to authenticate the
69.24 request using commercially reasonable efforts. In such cases, the controller may request	33.15 request using commercially reasonable efforts. In such cases, the controller may request
69.25 the provision of additional information reasonably necessary to authenticate the request. A	33.16 the provision of additional information reasonably necessary to authenticate the request. A
69.26 controller is not required to authenticate an opt-out request, but a controller may deny an	33.17 controller is not required to authenticate an opt-out request, but a controller may deny an
69.27 opt-out request if the controller has a good faith, reasonable, and documented belief that	33.18 opt-out request if the controller has a good faith, reasonable, and documented belief that
69.28 the request is fraudulent. If a controller denies an opt-out request because the controller	33.19 the request is fraudulent. If a controller denies an opt-out request because the controller
69.29 believes a request is fraudulent, the controller must notify the person who made the request	33.20 believes a request is fraudulent, the controller must notify the person who made the request
69.30 that the request was denied due to the controller's belief that the request was fraudulent and	33.21 that the request was denied due to the controller's belief that the request was fraudulent and
69.31 state the controller's basis for that belief.	33.22 state the controller's basis for that belief.
69.32 (i) In response to a consumer request under subdivision 1, a controller must not disclose	33.23 (i) In response to a consumer request under subdivision 1, a controller must not disclose
69.33 the following information about a consumer, but must instead inform the consumer with	33.24 the following information about a consumer, but must instead inform the consumer with
69.34 sufficient particularity that the controller has collected that type of information:	33.25 sufficient particularity that the controller has collected that type of information:
70.1 (1) Social Security number;	33.26 (1) Social Security number;
70.2 (2) driver's license number or other government-issued identification number;	33.27 (2) driver's license number or other government-issued identification number;
70.3 (3) financial account number;	33.28 (3) financial account number;
70.4 (4) health insurance account number or medical identification number;	33.29 (4) health insurance account number or medical identification number;
70.5 (5) account password, security questions, or answers; or	33.30 (5) account password, security questions, or answers; or
70.6 (6) biometric data.	33.31 (6) biometric data.
70.7 (j) In response to a consumer request under subdivision 1, a controller is not required	34.1 (j) In response to a consumer request under subdivision 1, a controller is not required
70.8 to reveal any trade secret.	34.2 to reveal any trade secret.
70.9 (k) A controller that has obtained personal data about a consumer from a source other	34.3 (k) A controller that has obtained personal data about a consumer from a source other
70.10 than the consumer may comply with a consumer's request to delete the consumer's personal	34.4 than the consumer may comply with a consumer's request to delete the consumer's personal
70.11 data pursuant to subdivision 1, paragraph (d), by either:	34.5 data pursuant to subdivision 1, paragraph (d), by either:
70.12 (1) retaining a record of the deletion request, retaining the minimum data necessary for	34.6 (1) retaining a record of the deletion request, retaining the minimum data necessary for
70.13 the purpose of ensuring the consumer's personal data remains deleted from the business's	34.7 the purpose of ensuring the consumer's personal data remains deleted from the business's

70.14 records, and not using the retained data for any other purpose pursuant to the provisions of
70.15 this chapter; or

70.16   (2) opting the consumer out of the processing of personal data for any purpose except
70.17 for the purposes exempted pursuant to the provisions of this chapter.

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

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

70.24   (c) Within 45 days of receipt of an appeal, a controller must inform the consumer of any
70.25 action taken or not taken in response to the appeal, along with a written explanation of the
70.26 reasons in support thereof. That period may be extended by 60 additional days where
70.27 reasonably necessary, taking into account the complexity and number of the requests serving
70.28 as the basis for the appeal. The controller must inform the consumer of any extension within
70.29 45 days of receipt of the appeal, together with the reasons for the delay.

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

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

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

71.9   (1) reidentify deidentified data;

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

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

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

34.8 records, and not using the retained data for any other purpose pursuant to the provisions of
34.9 this chapter; or

34.10   (2) opting the consumer out of the processing of personal data for any purpose except
34.11 for the purposes exempted pursuant to the provisions of this chapter.

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

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

34.18   (c) Within 45 days of receipt of an appeal, a controller must inform the consumer of any
34.19 action taken or not taken in response to the appeal, along with a written explanation of the
34.20 reasons in support thereof. That period may be extended by 60 additional days where
34.21 reasonably necessary, taking into account the complexity and number of the requests serving
34.22 as the basis for the appeal. The controller must inform the consumer of any extension within
34.23 45 days of receipt of the appeal, together with the reasons for the delay.

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

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

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

35.5   (1) reidentify deidentified data;

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

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

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

71.18 (ii) the controller does not use the personal data to recognize or respond to the specific	35.14 (ii) the controller does not use the personal data to recognize or respond to the specific
71.19 consumer who is the subject of the personal data, or associate the personal data with other	35.15 consumer who is the subject of the personal data, or associate the personal data with other
71.20 personal data about the same specific consumer; and	35.16 personal data about the same specific consumer; and
71.21 (iii) the controller does not sell the personal data to any third party or otherwise	35.17 (iii) the controller does not sell the personal data to any third party or otherwise
71.22 voluntarily disclose the personal data to any third party other than a processor, except as	35.18 voluntarily disclose the personal data to any third party other than a processor, except as
71.23 otherwise permitted in this section.	35.19 otherwise permitted in this section.
71.24 (b) The rights contained in section 325O.05, subdivision 1, paragraphs (b) to (h), do not	35.20 (b) The rights contained in section 325O.05, subdivision 1, paragraphs (b) to (h), do not
71.25 apply to pseudonymous data in cases where the controller is able to demonstrate any	35.21 apply to pseudonymous data in cases where the controller is able to demonstrate any
71.26 information necessary to identify the consumer is kept separately and is subject to effective	35.22 information necessary to identify the consumer is kept separately and is subject to effective
71.27 technical and organizational controls that prevent the controller from accessing the	35.23 technical and organizational controls that prevent the controller from accessing the
71.28 information.	35.24 information.
71.29 (c) A controller that uses pseudonymous data or deidentified data must exercise reasonable	35.25 (c) A controller that uses pseudonymous data or deidentified data must exercise reasonable
71.30 oversight to monitor compliance with any contractual commitments to which the	35.26 oversight to monitor compliance with any contractual commitments to which the
71.31 pseudonymous data or deidentified data are subject, and must take appropriate steps to	35.27 pseudonymous data or deidentified data are subject, and must take appropriate steps to
71.32 address any breaches of contractual commitments.	35.28 address any breaches of contractual commitments.
72.1 (d) A processor or third party must not attempt to identify the subjects of deidentified	35.29 (d) A processor or third party must not attempt to identify the subjects of deidentified
72.2 or pseudonymous data without the express authority of the controller that caused the data	35.30 or pseudonymous data without the express authority of the controller that caused the data
72.3 to be deidentified or pseudonymized.	35.31 to be deidentified or pseudonymized.
72.4 (e) A controller, processor, or third party must not attempt to identify the subjects of	36.1 (e) A controller, processor, or third party must not attempt to identify the subjects of
72.5 data that has been collected with only pseudonymous identifiers.	36.2 data that has been collected with only pseudonymous identifiers.
72.6 Sec. 8. **[325O.07] RESPONSIBILITIES OF CONTROLLERS.**	36.3 Sec. 8. **[325O.07] RESPONSIBILITIES OF CONTROLLERS.**
72.7 Subdivision 1. **Transparency obligations.** (a) Controllers must provide consumers with	36.4 Subdivision 1. **Transparency obligations.** (a) Controllers must provide consumers with
72.8 a reasonably accessible, clear, and meaningful privacy notice that includes:	36.5 a reasonably accessible, clear, and meaningful privacy notice that includes:
72.9 (1) the categories of personal data processed by the controller;	36.6 (1) the categories of personal data processed by the controller;
72.10 (2) the purposes for which the categories of personal data are processed;	36.7 (2) the purposes for which the categories of personal data are processed;
72.11 (3) an explanation of the rights contained in section 325O.05 and how and where	36.8 (3) an explanation of the rights contained in section 325O.05 and how and where
72.12 consumers may exercise those rights, including how a consumer may appeal a controller's	36.9 consumers may exercise those rights, including how a consumer may appeal a controller's
72.13 action with regard to the consumer's request;	36.10 action with regard to the consumer's request;
72.14 (4) the categories of personal data that the controller sells to or shares with third parties,	36.11 (4) the categories of personal data that the controller sells to or shares with third parties,
72.15 if any;	36.12 if any;
72.16 (5) the categories of third parties, if any, with whom the controller sells or shares personal	36.13 (5) the categories of third parties, if any, with whom the controller sells or shares personal
72.17 data;	36.14 data;
72.18 (6) the controller's contact information, including an active email address or other online	36.15 (6) the controller's contact information, including an active email address or other online
72.19 mechanism that the consumer may use to contact the controller;	36.16 mechanism that the consumer may use to contact the controller;

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

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

72.22   (b) If a controller sells personal data to third parties, processes personal data for targeted
72.23   advertising, or engages in profiling in furtherance of decisions that produce legal effects
72.24   concerning a consumer or similarly significant effects concerning a consumer, the controller
72.25   must disclose the processing in the privacy notice and provide access to a clear and
72.26   conspicuous method outside the privacy notice for a consumer to opt out of the sale,
72.27   processing, or profiling in furtherance of decisions that produce legal effects concerning a
72.28   consumer or similarly significant effects concerning a consumer. This method may include
72.29   but is not limited to an internet hyperlink clearly labeled "Your Opt-Out Rights" or "Your
72.30   Privacy Rights" that directly effectuates the opt-out request or takes consumers to a web
72.31   page where the consumer can make the opt-out request.

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

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

73.6   (e) Whenever a controller makes a material change to the controller's privacy notice or
73.7   practices, the controller must notify consumers affected by the material change with respect
73.8   to any prospectively collected personal data and provide a reasonable opportunity for
73.9   consumers to withdraw consent to any further materially different collection, processing,
73.10   or transfer of previously collected personal data under the changed policy. The controller
73.11   shall take all reasonable electronic measures to provide notification regarding material
73.12   changes to affected consumers, taking into account available technology and the nature of
73.13   the relationship.

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

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

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

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

36.19   (b) If a controller sells personal data to third parties, processes personal data for targeted
36.20   advertising, or engages in profiling in furtherance of decisions that produce legal effects
36.21   concerning a consumer or similarly significant effects concerning a consumer, the controller
36.22   must disclose the processing in the privacy notice and provide access to a clear and
36.23   conspicuous method outside the privacy notice for a consumer to opt out of the sale,
36.24   processing, or profiling in furtherance of decisions that produce legal effects concerning a
36.25   consumer or similarly significant effects concerning a consumer. This method may include
36.26   but is not limited to an Internet hyperlink clearly labeled "Your Opt-Out Rights" or "Your
36.27   Privacy Rights" that directly effectuates the opt-out request or takes consumers to a web
36.28   page where the consumer can make the opt-out request.

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

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

37.3   (e) Whenever a controller makes a material change to the controller's privacy notice or
37.4   practices, the controller must notify consumers affected by the material change with respect
37.5   to any prospectively collected personal data and provide a reasonable opportunity for
37.6   consumers to withdraw consent to any further materially different collection, processing,
37.7   or transfer of previously collected personal data under the changed policy. The controller
37.8   shall take all reasonable electronic measures to provide notification regarding material
37.9   changes to affected consumers, taking into account available technology and the nature of
37.10   the relationship.

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

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

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

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

73.32   (c) A controller shall establish, implement, and maintain reasonable administrative,
73.33   technical, and physical data security practices to protect the confidentiality, integrity, and
73.34   accessibility of personal data, including the maintenance of an inventory of the data that
74.1   must be managed to exercise these responsibilities. The data security practices shall be
74.2   appropriate to the volume and nature of the personal data at issue.

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

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

74.15   (f) A controller may not process the personal data of a consumer for purposes of targeted
74.16   advertising, or sell the consumer's personal data, without the consumer's consent, under
74.17   circumstances where the controller knows that the consumer is between the ages of 13 and
74.18   16.

74.19   (g) A controller may not retain personal data that is no longer relevant and reasonably
74.20   necessary in relation to the purposes for which the data were collected and processed, unless
74.21   retention of the data is otherwise required by law or permitted under section 325O.09.

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

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

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

37.29   (c) A controller shall establish, implement, and maintain reasonable administrative,
37.30   technical, and physical data security practices to protect the confidentiality, integrity, and
37.31   accessibility of personal data, including the maintenance of an inventory of the data that
37.32   must be managed to exercise these responsibilities. The data security practices shall be
37.33   appropriate to the volume and nature of the personal data at issue.

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

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

38.13   (f) A controller may not process the personal data of a consumer for purposes of targeted
38.14   advertising, or sell the consumer's personal data, without the consumer's consent, under
38.15   circumstances where the controller knows that the consumer is between the ages of 13 and
38.16   16.

38.17   (g) A controller may not retain personal data that is no longer relevant and reasonably
38.18   necessary in relation to the purposes for which the data were collected and processed, unless
38.19   retention of the data is otherwise required by law or permitted under section 325O.09.

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

74.29 (b) A controller may not discriminate against a consumer for exercising any of the rights 74.30 contained in this chapter, including denying goods or services to the consumer, charging 74.31 different prices or rates for goods or services, and providing a different level of quality of 74.32 goods and services to the consumer. This subdivision does not: (1) require a controller to 74.33 provide a good or service that requires the personal data of a consumer that the controller 74.34 does not collect or maintain; or (2) prohibit a controller from offering a different price, rate, 75.1 level, quality, or selection of goods or services to a consumer, including offering goods or 75.2 services for no fee, if the offering is in connection with a consumer's voluntary participation 75.3 in a bona fide loyalty, rewards, premium features, discounts, or club card program.	38.27 (b) A controller may not discriminate against a consumer for exercising any of the rights 38.28 contained in this chapter, including denying goods or services to the consumer, charging 38.29 different prices or rates for goods or services, and providing a different level of quality of 38.30 goods and services to the consumer. This subdivision does not: (1) require a controller to 38.31 provide a good or service that requires the consumer's personal data that the controller does 38.32 not collect or maintain; or (2) prohibit a controller from offering a different price, rate, level, 38.33 quality, or selection of goods or services to a consumer, including offering goods or services 39.1 for no fee, if the offering is in connection with a consumer's voluntary participation in a 39.2 bona fide loyalty, rewards, premium features, discounts, or club card program.
75.4 (c) A controller may not sell personal data to a third-party controller as part of a bona 75.5 fide loyalty, rewards, premium features, discounts, or club card program under paragraph 75.6 (b) unless:	39.3 (c) A controller may not sell personal data to a third-party controller as part of a bona 39.4 fide loyalty, rewards, premium features, discounts, or club card program under paragraph 39.5 (b) unless:
75.7 (1) the sale is reasonably necessary to enable the third party to provide a benefit to which 75.8 the consumer is entitled;	39.6 (1) the sale is reasonably necessary to enable the third party to provide a benefit to which 39.7 the consumer is entitled;
75.9 (2) the sale of personal data to third parties is clearly disclosed in the terms of the 75.10 program; and	39.8 (2) the sale of personal data to third parties is clearly disclosed in the terms of the 39.9 program; and
75.11 (3) the third party uses the personal data only for purposes of facilitating a benefit to 75.12 which the consumer is entitled and does not retain or otherwise use or disclose the personal 75.13 data for any other purpose.	39.10 (3) the third party uses the personal data only for purposes of facilitating a benefit to 39.11 which the consumer is entitled and does not retain or otherwise use or disclose the personal 39.12 data for any other purpose.
75.14 Subd. 4. **Waiver of rights unenforceable.** Any provision of a contract or agreement of 75.15 any kind that purports to waive or limit in any way a consumer's rights under this chapter 75.16 is contrary to public policy and is void and unenforceable.	39.13 Subd. 4. **Waiver of rights unenforceable.** Any provision of a contract or agreement of 39.14 any kind that purports to waive or limit in any way a consumer's rights under this chapter 39.15 is contrary to public policy and is void and unenforceable.
75.17 Sec. 9. **[325O.075] REQUIREMENTS FOR SMALL BUSINESSES.**	39.16 Sec. 9. **[325O.075] REQUIREMENTS FOR SMALL BUSINESSES.**
75.18 (a) A small business, as defined by the United States Small Business Administration 75.19 under Code of Federal Regulations, title 13, part 121, that conducts business in Minnesota 75.20 or produces products or services that are targeted to residents of Minnesota, must not sell 75.21 a consumer's sensitive data without the consumer's prior consent.	39.17 (a) A small business, as defined by the United States Small Business Administration 39.18 under Code of Federal Regulations, title 13, part 121, that conducts business in Minnesota 39.19 or produces products or services that are targeted to residents of Minnesota, must not sell 39.20 a consumer's sensitive data without the consumer's prior consent.
75.22 (b) Penalties and attorney general enforcement procedures under section 325O.10 apply 75.23 to a small business that violates this section.	39.21 (b) Penalties and attorney general enforcement procedures under section 325O.10 apply 39.22 to a small business that violates this section.
75.24 Sec. 10. **[325O.08] DATA PRIVACY POLICIES AND DATA PRIVACY** 75.25 **PROTECTION ASSESSMENTS.**	39.23 Sec. 10. **[325O.08] DATA PRIVACY POLICIES AND DATA PRIVACY AND** 39.24 **PROTECTION ASSESSMENTS.**
75.26 (a) A controller must document and maintain a description of the policies and procedures 75.27 the controller has adopted to comply with this chapter. The description must include, where 75.28 applicable:	39.25 (a) A controller must document and maintain a description of the policies and procedures 39.26 the controller has adopted to comply with this chapter. The description must include, where 39.27 applicable:

75.29 (1) the name and contact information for the controller's chief privacy officer or other 75.30 individual with primary responsibility for directing the policies and procedures implemented 75.31 to comply with the provisions of this chapter; and	39.28 (1) the name and contact information for the controller's chief privacy officer or other 39.29 individual with primary responsibility for directing the policies and procedures implemented 39.30 to comply with the provisions of this chapter; and
76.1 (2) a description of the controller's data privacy policies and procedures which reflect 76.2 the requirements in section 325O.07, and any policies and procedures designed to:	40.1 (2) a description of the controller's data privacy policies and procedures which reflect 40.2 the requirements in section 325O.07, and any policies and procedures designed to:
76.3 (i) reflect the requirements of this chapter in the design of the controller's systems;	40.3 (i) reflect the requirements of this chapter in the design of the controller's systems;
76.4 (ii) identify and provide personal data to a consumer as required by this chapter;	40.4 (ii) identify and provide personal data to a consumer as required by this chapter;
76.5 (iii) establish, implement, and maintain reasonable administrative, technical, and physical 76.6 data security practices to protect the confidentiality, integrity, and accessibility of personal 76.7 data, including the maintenance of an inventory of the data that must be managed to exercise 76.8 the responsibilities under this item;	40.5 (iii) establish, implement, and maintain reasonable administrative, technical, and physical 40.6 data security practices to protect the confidentiality, integrity, and accessibility of personal 40.7 data, including the maintenance of an inventory of the data that must be managed to exercise 40.8 the responsibilities under this item;
76.9 (iv) limit the collection of personal data to what is adequate, relevant, and reasonably 76.10 necessary in relation to the purposes for which the data are processed;	40.9 (iv) limit the collection of personal data to what is adequate, relevant, and reasonably 40.10 necessary in relation to the purposes for which the data are processed;
76.11 (v) prevent the retention of personal data that is no longer relevant and reasonably 76.12 necessary in relation to the purposes for which the data were collected and processed, unless 76.13 retention of the data is otherwise required by law or permitted under section 325O.09; and	40.11 (v) prevent the retention of personal data that is no longer relevant and reasonably 40.12 necessary in relation to the purposes for which the data were collected and processed, unless 40.13 retention of the data is otherwise required by law or permitted under section 325O.09; and
76.14 (vi) identify and remediate violations of this chapter.	40.14 (vi) identify and remediate violations of this chapter.
76.15 (b) A controller must conduct and document a data privacy and protection assessment 76.16 for each of the following processing activities involving personal data:	40.15 (b) A controller must conduct and document a data privacy and protection assessment 40.16 for each of the following processing activities involving personal data:
76.17 (1) the processing of personal data for purposes of targeted advertising;	40.17 (1) the processing of personal data for purposes of targeted advertising;
76.18 (2) the sale of personal data;	40.18 (2) the sale of personal data;
76.19 (3) the processing of sensitive data;	40.19 (3) the processing of sensitive data;
76.20 (4) any processing activities involving personal data that present a heightened risk of 76.21 harm to consumers; and	40.20 (4) any processing activities involving personal data that present a heightened risk of 40.21 harm to consumers; and
76.22 (5) the processing of personal data for purposes of profiling, where the profiling presents 76.23 a reasonably foreseeable risk of:	40.22 (5) the processing of personal data for purposes of profiling, where the profiling presents 40.23 a reasonably foreseeable risk of:
76.24 (i) unfair or deceptive treatment of, or disparate impact on, consumers;	40.24 (i) unfair or deceptive treatment of, or disparate impact on, consumers;
76.25 (ii) financial, physical, or reputational injury to consumers;	40.25 (ii) financial, physical, or reputational injury to consumers;
76.26 (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or 76.27 concerns, of consumers, where the intrusion would be offensive to a reasonable person; or	40.26 (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or 40.27 concerns, of consumers, where the intrusion would be offensive to a reasonable person; or
76.28 (iv) other substantial injury to consumers.	40.28 (iv) other substantial injury to consumers.

77.1 (c) A data privacy and protection assessment must take into account the type of personal 77.2 data to be processed by the controller, including the extent to which the personal data are 77.3 sensitive data, and the context in which the personal data are to be processed.	41.1 (c) A data privacy and protection assessment must take into account the type of personal 41.2 data to be processed by the controller, including the extent to which the personal data are 41.3 sensitive data, and the context in which the personal data are to be processed.
77.4 (d) A data privacy and protection assessment must identify and weigh the benefits that 77.5 may flow directly and indirectly from the processing to the controller, consumer, other 77.6 stakeholders, and the public against the potential risks to the rights of the consumer associated 77.7 with the processing, as mitigated by safeguards that can be employed by the controller to 77.8 reduce the potential risks. The use of deidentified data and the reasonable expectations of 77.9 consumers, as well as the context of the processing and the relationship between the controller 77.10 and the consumer whose personal data will be processed, must be factored into this 77.11 assessment by the controller.	41.4 (d) A data privacy and protection assessment must identify and weigh the benefits that 41.5 may flow directly and indirectly from the processing to the controller, consumer, other 41.6 stakeholders, and the public against the potential risks to the rights of the consumer associated 41.7 with the processing, as mitigated by safeguards that can be employed by the controller to 41.8 reduce the potential risks. The use of deidentified data and the reasonable expectations of 41.9 consumers, as well as the context of the processing and the relationship between the controller 41.10 and the consumer whose personal data will be processed, must be factored into this 41.11 assessment by the controller.
77.12 (e) A data privacy and protection assessment must include the description of policies 77.13 and procedures required by paragraph (a).	41.12 (e) A data privacy and protection assessment must include the description of policies 41.13 and procedures required by paragraph (a).
77.14 (f) As part of a civil investigative demand, the attorney general may request, in writing, 77.15 that a controller disclose any data privacy and protection assessment that is relevant to an 77.16 investigation conducted by the attorney general. The controller must make a data privacy 77.17 and protection assessment available to the attorney general upon a request made under this 77.18 paragraph. The attorney general may evaluate the data privacy and protection assessments 77.19 for compliance with this chapter. Data privacy and protection assessments are classified as 77.20 nonpublic data, as defined by section 13.02, subdivision 9. The disclosure of a data privacy 77.21 and protection assessment pursuant to a request from the attorney general under this 77.22 paragraph does not constitute a waiver of the attorney-client privilege or work product 77.23 protection with respect to the assessment and any information contained in the assessment.	41.14 (f) As part of a civil investigative demand, the attorney general may request, in writing, 41.15 that a controller disclose any data privacy and protection assessment that is relevant to an 41.16 investigation conducted by the attorney general. The controller must make a data privacy 41.17 and protection assessment available to the attorney general upon a request made under this 41.18 paragraph. The attorney general may evaluate the data privacy and protection assessments 41.19 for compliance with this chapter. Data privacy and protection assessments are classified as 41.20 nonpublic data, as defined by section 13.02, subdivision 9. The disclosure of a data privacy 41.21 and protection assessment pursuant to a request from the attorney general under this 41.22 paragraph does not constitute a waiver of the attorney-client privilege or work product 41.23 protection with respect to the assessment and any information contained in the assessment.
77.24 (g) Data privacy and protection assessments or risk assessments conducted by a controller 77.25 for the purpose of compliance with other laws or regulations may qualify under this section 77.26 if the assessments have a similar scope and effect.	41.24 (g) Data privacy and protection assessments or risk assessments conducted by a controller 41.25 for the purpose of compliance with other laws or regulations may qualify under this section 41.26 if the assessments have a similar scope and effect.
77.27 (h) A single data protection assessment may address multiple sets of comparable 77.28 processing operations that include similar activities.	41.27 (h) A single data protection assessment may address multiple sets of comparable 41.28 processing operations that include similar activities.
77.29 Sec. 11. **[325O.09] LIMITATIONS AND APPLICABILITY.**	41.29 Sec. 11. **[325O.09] LIMITATIONS AND APPLICABILITY.**
77.30 (a) The obligations imposed on controllers or processors under this chapter do not restrict 77.31 a controller's or a processor's ability to:	41.30 (a) The obligations imposed on controllers or processors under this chapter do not restrict 41.31 a controller's or a processor's ability to:
78.1 (1) comply with federal, state, or local laws, rules, or regulations, including but not 78.2 limited to data retention requirements in state or federal law notwithstanding a consumer's 78.3 request to delete personal data;	42.1 (1) comply with federal, state, or local laws, rules, or regulations, including but not 42.2 limited to data retention requirements in state or federal law notwithstanding a consumer's 42.3 request to delete personal data;
78.4 (2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or 78.5 summons by federal, state, local, or other governmental authorities;	42.4 (2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or 42.5 summons by federal, state, local, or other governmental authorities;

78.6 (3) cooperate with law enforcement agencies concerning conduct or activity that the 78.7 controller or processor reasonably and in good faith believes may violate federal, state, or 78.8 local laws, rules, or regulations;	42.6 (3) cooperate with law enforcement agencies concerning conduct or activity that the 42.7 controller or processor reasonably and in good faith believes may violate federal, state, or 42.8 local laws, rules, or regulations;
78.9 (4) investigate, establish, exercise, prepare for, or defend legal claims;	42.9 (4) investigate, establish, exercise, prepare for, or defend legal claims;
78.10 (5) provide a product or service specifically requested by a consumer, perform a contract 78.11 to which the consumer is a party, including fulfilling the terms of a written warranty, or 78.12 take steps at the request of the consumer prior to entering into a contract;	42.10 (5) provide a product or service specifically requested by a consumer; perform a contract 42.11 to which the consumer is a party, including fulfilling the terms of a written warranty; or 42.12 take steps at the request of the consumer prior to entering into a contract;
78.13 (6) take immediate steps to protect an interest that is essential for the life or physical 78.14 safety of the consumer or of another natural person, and where the processing cannot be 78.15 manifestly based on another legal basis;	42.13 (6) take immediate steps to protect an interest that is essential for the life or physical 42.14 safety of the consumer or of another natural person, and where the processing cannot be 42.15 manifestly based on another legal basis;
78.16 (7) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, 78.17 harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity 78.18 or security of systems; or investigate, report, or prosecute those responsible for any such 78.19 action;	42.16 (7) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, 42.17 harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity 42.18 or security of systems; or investigate, report, or prosecute those responsible for any such 42.19 action;
78.20 (8) assist another controller, processor, or third party with any of the obligations under 78.21 this paragraph;	42.20 (8) assist another controller, processor, or third party with any of the obligations under 42.21 this paragraph;
78.22 (9) engage in public or peer-reviewed scientific, historical, or statistical research in the 78.23 public interest that adheres to all other applicable ethics and privacy laws and is approved, 78.24 monitored, and governed by an institutional review board, human subjects research ethics 78.25 review board, or a similar independent oversight entity which has determined that:	42.22 (9) engage in public or peer-reviewed scientific, historical, or statistical research in the 42.23 public interest that adheres to all other applicable ethics and privacy laws and is approved, 42.24 monitored, and governed by an institutional review board, human subjects research ethics 42.25 review board, or a similar independent oversight entity that has determined:
78.26 (i) the research is likely to provide substantial benefits that do not exclusively accrue to 78.27 the controller;	42.26 (i) the research is likely to provide substantial benefits that do not exclusively accrue to 42.27 the controller;
78.28 (ii) the expected benefits of the research outweigh the privacy risks; and	42.28 (ii) the expected benefits of the research outweigh the privacy risks; and
78.29 (iii) the controller has implemented reasonable safeguards to mitigate privacy risks 78.30 associated with research, including any risks associated with reidentification; or	42.29 (iii) the controller has implemented reasonable safeguards to mitigate privacy risks 42.30 associated with research, including any risks associated with reidentification; or
78.31 (10) process personal data for the benefit of the public in the areas of public health, 78.32 community health, or population health, but only to the extent that the processing is:	42.31 (10) process personal data for the benefit of the public in the areas of public health, 42.32 community health, or population health, but only to the extent that the processing is:
79.1 (i) subject to suitable and specific measures to safeguard the rights of the consumer 79.2 whose personal data is being processed; and	43.1 (i) subject to suitable and specific measures to safeguard the rights of the consumer 43.2 whose personal data is being processed; and
79.3 (ii) under the responsibility of a professional individual who is subject to confidentiality 79.4 obligations under federal, state, or local law.	43.3 (ii) under the responsibility of a professional individual who is subject to confidentiality 43.4 obligations under federal, state, or local law.
79.5 (b) The obligations imposed on controllers or processors under this chapter do not restrict 79.6 a controller's or processor's ability to collect, use, or retain data to:	43.5 (b) The obligations imposed on controllers or processors under this chapter do not restrict 43.6 a controller's or processor's ability to collect, use, or retain data to:

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

79.9   (2) perform internal operations that are reasonably aligned with the expectations of the
79.10 consumer based on the consumer's existing relationship with the controller, or are otherwise
79.11 compatible with processing in furtherance of the provision of a product or service specifically
79.12 requested by a consumer or the performance of a contract to which the consumer is a party;
79.13 or

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

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

79.21   (d) A controller or processor that discloses personal data to a third-party controller or
79.22 processor in compliance with the requirements of this chapter is not in violation of this
79.23 chapter if the recipient processes the personal data in violation of this chapter, provided that
79.24 at the time of disclosing the personal data, the disclosing controller or processor did not
79.25 have actual knowledge that the recipient intended to commit a violation. A third-party
79.26 controller or processor receiving personal data from a controller or processor in compliance
79.27 with the requirements of this chapter is not in violation of this chapter for the obligations
79.28 of the controller or processor from which the third-party controller or processor receives
79.29 the personal data.

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

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

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

80.3   (f) Personal data that are processed by a controller pursuant to this section may be
80.4   processed solely to the extent that the processing is:

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

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

80.8   (3) insofar as possible, taking into account the nature and purpose of processing the
80.9   personal data, subjected to reasonable administrative, technical, and physical measures to

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

43.9   (2) perform internal operations that are reasonably aligned with the expectations of the
43.10 consumer based on the consumer's existing relationship with the controller, or are otherwise
43.11 compatible with processing in furtherance of the provision of a product or service specifically
43.12 requested by a consumer or the performance of a contract to which the consumer is a party;
43.13 or

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

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

43.21   (d) A controller or processor that discloses personal data to a third-party controller or
43.22 processor in compliance with the requirements of this chapter is not in violation of this
43.23 chapter if the recipient processes the personal data in violation of this chapter, provided that
43.24 at the time of disclosing the personal data, the disclosing controller or processor did not
43.25 have actual knowledge that the recipient intended to commit a violation. A third-party
43.26 controller or processor receiving personal data from a controller or processor in compliance
43.27 with the requirements of this chapter is not in violation of this chapter for the obligations
43.28 of the controller or processor from which the third-party controller or processor receives
43.29 the personal data.

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

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

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

44.3   (f) Personal data that are processed by a controller pursuant to this section may be
44.4   processed solely to the extent that the processing is:

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

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

44.8   (3) insofar as possible, taking into account the nature and purpose of processing the
44.9   personal data, subjected to reasonable administrative, technical, and physical measures to

80.10 protect the confidentiality, integrity, and accessibility of the personal data, and to reduce 80.11 reasonably foreseeable risks of harm to consumers.	44.10 protect the confidentiality, integrity, and accessibility of the personal data, and to reduce 44.11 reasonably foreseeable risks of harm to consumers.
80.12 (g) If a controller processes personal data pursuant to an exemption in this section, the 80.13 controller bears the burden of demonstrating that the processing qualifies for the exemption 80.14 and complies with the requirements in paragraph (f).	44.12 (g) If a controller processes personal data pursuant to an exemption in this section, the 44.13 controller bears the burden of demonstrating that the processing qualifies for the exemption 44.14 and complies with the requirements in paragraph (f).
80.15 (h) Processing personal data solely for the purposes expressly identified in paragraph 80.16 (a), clauses (1) to (7), does not, by itself, make an entity a controller with respect to the 80.17 processing.	44.15 (h) Processing personal data solely for the purposes expressly identified in paragraph 44.16 (a), clauses (1) to (7), does not, by itself, make an entity a controller with respect to the 44.17 processing.
80.18 Sec. 12. **[325O.10] ATTORNEY GENERAL ENFORCEMENT.**	44.18 Sec. 12. **[325O.10] ATTORNEY GENERAL ENFORCEMENT.**
80.19 (a) In the event that a controller or processor violates this chapter, the attorney general, 80.20 prior to filing an enforcement action under paragraph (b), must provide the controller or 80.21 processor with a warning letter identifying the specific provisions of this chapter the attorney 80.22 general alleges have been or are being violated. If, after 30 days of issuance of the warning 80.23 letter, the attorney general believes the controller or processor has failed to cure any alleged 80.24 violation, the attorney general may bring an enforcement action under paragraph (b). This 80.25 paragraph expires January 31, 2026.	44.19 (a) In the event that a controller or processor violates this chapter, the attorney general, 44.20 prior to filing an enforcement action under paragraph (b), must provide the controller or 44.21 processor with a warning letter identifying the specific provisions of this chapter the attorney 44.22 general alleges have been or are being violated. If, after 30 days of issuance of the warning 44.23 letter, the attorney general believes the controller or processor has failed to cure any alleged 44.24 violation, the attorney general may bring an enforcement action under paragraph (b). This 44.25 paragraph expires January 31, 2026.
80.26 (b) The attorney general may bring a civil action against a controller or processor to 80.27 enforce a provision of this chapter in accordance with section 8.31. If the state prevails in 80.28 an action to enforce this chapter, the state may, in addition to penalties provided by paragraph 80.29 (c) or other remedies provided by law, be allowed an amount determined by the court to be 80.30 the reasonable value of all or part of the state's litigation expenses incurred.	44.26 (b) The attorney general may bring a civil action against a controller or processor to 44.27 enforce a provision of this chapter in accordance with section 8.31. If the state prevails in 44.28 an action to enforce this chapter, the state may, in addition to penalties provided by paragraph 44.29 (c) or other remedies provided by law, be allowed an amount determined by the court to be 44.30 the reasonable value of all or part of the state's litigation expenses incurred.
80.31 (c) Any controller or processor that violates this chapter is subject to an injunction and 80.32 liable for a civil penalty of not more than $7,500 for each violation.	44.31 (c) Any controller or processor that violates this chapter is subject to an injunction and 44.32 liable for a civil penalty of not more than $7,500 for each violation.
81.1 (d) Nothing in this chapter establishes a private right of action, including under section 81.2 8.31, subdivision 3a, for a violation of this chapter or any other law.	45.1 (d) Nothing in this chapter establishes a private right of action, including under section 45.2 8.31, subdivision 3a, for a violation of this chapter or any other law.
81.3 Sec. 13. **[325O.11] PREEMPTION OF LOCAL LAW; SEVERABILITY.**	45.3 Sec. 13. **[325O.11] PREEMPTION OF LOCAL LAW; SEVERABILITY.**
81.4 (a) This chapter supersedes and preempts laws, ordinances, regulations, or the equivalent 81.5 adopted by any local government regarding the processing of personal data by controllers 81.6 or processors.	45.4 (a) This chapter supersedes and preempts laws, ordinances, regulations, or the equivalent 45.5 adopted by any local government regarding the processing of personal data by controllers 45.6 or processors.
81.7 (b) If any provision of this chapter or this chapter's application to any person or 81.8 circumstance is held invalid, the remainder of this chapter or the application of the provision 81.9 to other persons or circumstances is not affected.	45.7 (b) If any provision of this chapter or the chapter's application to any person or 45.8 circumstance is held invalid, the remainder of the chapter or the application of the provision 45.9 to other persons or circumstances is not affected.

81.10   Sec. 14. **EFFECTIVE DATE.**

81.11   This article is effective July 31, 2025, except that postsecondary institutions regulated
81.12   by the Office of Higher Education are not required to comply with this article until July 31,
81.13   2029.

45.10   Sec. 14. **EFFECTIVE DATE.**

45.11   This article is effective July 31, 2025, except that postsecondary institutions regulated
45.12   by the Office of Higher Education are not required to comply with this article until July 31,
45.13   2029.