

SENATE
STATE OF MINNESOTA
NINETY-THIRD SESSION

S.F. No. 5301

(SENATE AUTHORS: KLEIN)		
DATE	D-PG	OFFICIAL STATUS
04/04/2024	13374	Introduction and first reading
		Referred to Commerce and Consumer Protection
04/18/2024	14198a	Comm report: To pass as amended and re-refer to Finance

1.1

A bill for an act

1.2

relating to commerce; modifying appropriations to the Office of Cannabis

1.3

Management and the Department of Health; modifying fees assessed by the

1.4

Department of Commerce; adding the Minnesota Consumer Data Privacy Act;

1.5

adding and modifying consumer protection provisions; amending Minnesota

1.6

Statutes 2022, sections 45.0135, subdivision 7; 62Q.73, subdivision 3; 325E.21,

1.7

by adding a subdivision; Minnesota Statutes 2023 Supplement, sections 144.197;

1.8

325E.21, subdivision 1b; 342.72; Laws 2023, chapter 63, article 9, sections 5; 10;

1.9

15, subdivision 4; 20; proposing coding for new law in Minnesota Statutes, chapters

1.10

13; 58B; 62J; proposing coding for new law as Minnesota Statutes, chapter 325O.

1.11

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

1.12

ARTICLE 1

1.13

APPROPRIATIONS

1.14

Section 1. Laws 2023, chapter 63, article 9, section 5, is amended to read:

1.15

Sec. 5. OFFICE OF CANNABIS

1.16

MANAGEMENT

\$21,614,000\$17,953,00020,680,000

1.17

The base for this appropriation is ~~\$35,587,000~~

1.18

\$36,909,000 in fiscal year 2026 and

1.19

~~\$38,144,000~~ \$39,530,000 in fiscal year 2027.

1.20

\$1,000,000 the second year is for cannabis

1.21

industry community renewal grants under

1.22

Minnesota Statutes, section 342.70. Of these

1.23

amounts, up to three percent may be used for

1.24

administrative expenses. The base for this

2.1 appropriation is \$15,000,000 in fiscal year
2.2 2026 and each fiscal year thereafter.

2.3 \$1,000,000 each year is for transfer to the
2.4 CanGrow revolving loan account established
2.5 under Minnesota Statutes, section 342.73,
2.6 subdivision 4. Of these amounts, up to three
2.7 percent may be used for administrative
2.8 expenses.

2.9 \$1,107,000 the second year is for temporary
2.10 regulation under the Health Enforcement
2.11 Consolidation Act of 1993 of edible products
2.12 extracted from hemp. This is a onetime
2.13 appropriation.

2.14 \$771,000 the second year is for testing
2.15 products regulated under Minnesota Statutes,
2.16 section 151.72, and chapter 342. The base for
2.17 this appropriation is \$690,000 in fiscal year
2.18 2026 and each year thereafter.

2.19 \$849,000 the second year is for the Office of
2.20 Cannabis Management to operate a state
2.21 reference laboratory. The base for this
2.22 appropriation is \$632,000 in fiscal year 2026
2.23 and \$696,000 in fiscal year 2027.

2.24 Sec. 2. Laws 2023, chapter 63, article 9, section 10, is amended to read:

2.25 Sec. 10. **HEALTH**

2.26				<u>20,252,000</u>
2.27	Subdivision 1. Total Appropriation	\$	3,300,000	\$ <u>23,025,000</u>

2.28 The base for this appropriation is ~~\$19,064,000~~
2.29 \$23,242,000 in fiscal year 2026 and ~~each fiscal~~
2.30 ~~year thereafter~~ \$23,178,000 in fiscal year
2.31 2027.

3.1 The amounts that may be spent for each
 3.2 purpose are specified in the following
 3.3 subdivisions.

3.4	Subd. 2. <u>Youth Prevention and Education</u>		5,000,000
3.5	<u>Program</u>	-0-	<u>4,363,000</u>

3.6 For administration and grants under Minnesota
 3.7 Statutes, section 144.197, subdivision 1. Of
 3.8 the amount appropriated, \$2,863,000 is for
 3.9 program operations and administration and
 3.10 \$1,500,000 is for grants. The base for this
 3.11 appropriation is \$4,534,000 in fiscal year 2026
 3.12 and \$4,470,000 in fiscal year 2027.

3.13	Subd. 3. <u>Prevention and Education Grants for</u>		2,000,000
3.14	<u>Pregnant or Breastfeeding Individuals</u>	-0-	<u>1,788,000</u>

3.15 For ~~grants under~~ a coordinated prevention and
 3.16 education program for pregnant and
 3.17 breastfeeding individuals under Minnesota
 3.18 Statutes, section 144.197, subdivision 2. The
 3.19 base for this appropriation is \$1,834,000 in
 3.20 fiscal year 2026 and each year thereafter.

3.21	Subd. 4. Local and Tribal Health Departments	-0-	10,000,000
------	---	-----	------------

3.22 For administration and grants under Minnesota
 3.23 Statutes, section 144.197, subdivision 4. Of
 3.24 the amount appropriated, \$1,094,000 is for
 3.25 administration and \$8,906,000 is for grants.

3.26	Subd. 5. Cannabis Data Collection and Biennial		
3.27	Reports	493,000	493,000

3.28 For reports under Minnesota Statutes, section
 3.29 144.196.

3.30	Subd. 6. Administration for Expungement		
3.31	Orders	71,000	71,000

3.32 For administration related to orders issued by
 3.33 the Cannabis Expungement Board. The base
 3.34 for this appropriation is \$71,000 in fiscal year

4.1	2026, \$71,000 in fiscal year 2027, \$71,000 in		
4.2	fiscal year 2028, \$71,000 in fiscal year 2029,		
4.3	and \$0 in fiscal year 2030.		
4.4	Subd. 7. Grants to the Minnesota Poison Control		
4.5	System	910,000	810,000
4.6	For <u>administration and grants under Minnesota</u>		
4.7	<u>Statutes, section 145.93. Of the amount</u>		
4.8	<u>appropriated in fiscal year 2025, \$15,000 is</u>		
4.9	<u>for administration and \$795,000 is for grants.</u>		
4.10	Subd. 8. Temporary Regulation of Edible		
4.11	Products Extracted from Hemp	1,107,000	1,107,000 -0-
4.12	For temporary regulation under the health		
4.13	enforcement consolidation act of edible		
4.14	products extracted from hemp. <u>The</u>		
4.15	<u>commissioner may transfer encumbrances and</u>		
4.16	<u>unobligated amounts from fiscal year 2024 to</u>		
4.17	<u>the Office of Cannabis Management for this</u>		
4.18	<u>purpose.</u> This is a onetime appropriation.		
4.19	Subd. 9. Testing:	719,000	771,000 -0-
4.20	For testing of edible cannabinoid products.		
4.21	The base for this appropriation is \$690,000 in		
4.22	fiscal year 2026 and each fiscal year thereafter.		
4.23	<u>The commissioner may transfer encumbrances</u>		
4.24	<u>and unobligated amounts from fiscal year 2024</u>		
4.25	<u>to the Office of Cannabis Management for this</u>		
4.26	<u>purpose.</u>		
4.27	<u>Subd. 10. Substance Use Treatment, Recovery,</u>		
4.28	<u>and Prevention</u>	-0-	<u>5,500,000</u>
4.29	<u>For the purposes outlined in Minnesota</u>		
4.30	<u>Statutes, section 342.72. The base for this</u>		
4.31	<u>appropriation is \$5,500,000 in fiscal year 2026</u>		
4.32	<u>and each fiscal year thereafter.</u>		
4.33	<u>EFFECTIVE DATE. This section is effective the day following final enactment.</u>		

5.1 Sec. 3. Laws 2023, chapter 63, article 9, section 15, subdivision 4, is amended to read:

5.2 Subd. 4. **Office of Traffic and Safety** 11,485,000 6,117,000

5.3 (a) The base for this appropriation is
 5.4 \$5,000,000 in fiscal year 2026 and each fiscal
 5.5 year thereafter.

5.6 (b) \$10,000,000 the first year and \$5,000,000
 5.7 the second year are for the drug evaluation
 5.8 and classification program for drug recognition
 5.9 evaluator training; additional phlebotomists;
 5.10 drug recognition training for peace officers,
 5.11 as defined in Minnesota Statutes, section
 5.12 626.84, subdivision 1, paragraph (c); and
 5.13 required continuing education training for drug
 5.14 recognition experts, program administration,
 5.15 grants to local law enforcement divisions, and
 5.16 making grants to eligible employers for drug
 5.17 evaluation and classification training costs of
 5.18 their staff. The commissioner must make
 5.19 reasonable efforts to reflect the geographic
 5.20 diversity of the state in making expenditures
 5.21 under this appropriation. This appropriation
 5.22 is available until June 30, 2027.

5.23 (c) \$1,485,000 the first year and \$1,117,000
 5.24 the second year are for a roadside testing pilot
 5.25 project. These are onetime appropriations.

5.26 **EFFECTIVE DATE.** This section is effective the day following final enactment.

5.27 Sec. 4. Laws 2023, chapter 63, article 9, section 20, is amended to read:

5.28 Sec. 20. **TRANSFERS.**

5.29 ~~(a)~~ \$1,000,000 in fiscal year 2024 and \$1,000,000 in fiscal year 2025 are transferred
 5.30 from the general fund to the dual training account in the special revenue fund under
 5.31 Minnesota Statutes, section 136A.246, subdivision 10, for grants to employers in the legal
 5.32 cannabis industry. The base for this transfer is \$1,000,000 in fiscal year 2026 and each fiscal

year thereafter. The commissioner may use up to six percent of the amount transferred for administrative costs. The commissioner shall give priority to applications from employers who are, or who are training employees who are, eligible to be social equity applicants under Minnesota Statutes, section 342.17. After June 30, 2025, any unencumbered balance from this transfer may be used for grants to any eligible employer under Minnesota Statutes, section 136A.246.

~~(b) \$5,500,000 in fiscal year 2024 and \$5,500,000 in fiscal year 2025 are transferred from the general fund to the substance use treatment, recovery, and prevention grant account established under Minnesota Statutes, section 342.72. The base for this transfer is \$5,500,000 in fiscal year 2026 and each fiscal year thereafter.~~

EFFECTIVE DATE. This section is effective the day following final enactment.

Sec. 5. **DEPARTMENT OF COMMERCE.**

The general fund base for the commissioner of commerce is increased by \$47,000 in fiscal year 2026 and each year thereafter for the commissioner of commerce to administer and enforce Minnesota Statutes, section 325E.21, subdivision 2c.

Sec. 6. **ATTORNEY GENERAL.**

The general fund base for the attorney general is increased by \$941,000 in fiscal year 2026 and \$701,000 in fiscal year 2027 to enforce the Minnesota Consumer Data Privacy Act under Minnesota Statutes, chapter 325O.

ARTICLE 2

MINNESOTA CONSUMER DATA PRIVACY ACT

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

Subdivision 1. **Scope.** The sections referred to in this section are 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."

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

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

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

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

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

7.17 (1) a digital or physical photograph;

7.18 (2) an audio or video recording; or

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.28 (p) "Personal data" means any information that is linked or reasonably linkable to an
8.29 identified or identifiable natural person. Personal data does not include deidentified data or
8.30 publicly available information. For purposes of this paragraph, "publicly available
8.31 information" means information that (1) is lawfully made available from federal, state, or

9.1 local government records or widely distributed media, or (2) a controller has a reasonable
9.2 basis to believe has lawfully been made available to the general public.

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

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

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

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

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

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

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

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

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

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

9.30 (6) the exchange of personal data between the producer of a good or service and
9.31 authorized agents of the producer who sell and service the goods and services, to enable

10.1 the cooperative provisioning of goods and services by both the producer and the producer's
10.2 agents.

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

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

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

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

10.9 (4) specific geolocation data.

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

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

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

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

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

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

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

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

11.4 Sec. 4. **[325O.03] SCOPE; EXCLUSIONS.**

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

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

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

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

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

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

11.19 (2) a federally recognized Indian tribe;

11.20 (3) information that meets the definition of:

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

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

11.24 (iii) patient identifying information for purposes of Code of Federal Regulations, title
11.25 42, part 2, established pursuant to United States Code, title 42, section 290dd-2;

11.26 (iv) identifiable private information for purposes of the federal policy for the protection
11.27 of human subjects, Code of Federal Regulations, title 45, part 46; identifiable private
11.28 information that is otherwise information collected as part of human subjects research
11.29 pursuant to the good clinical practice guidelines issued by the International Council for
11.30 Harmonisation; the protection of human subjects under Code of Federal Regulations, title

12.1 21, parts 50 and 56; or personal data used or shared in research conducted in accordance
12.2 with one or more of the requirements set forth in this paragraph;

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

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

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

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

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

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

12.15 (iii) a program or a qualified service organization, as defined by Code of Federal
12.16 Regulations, title 42, part 2, established pursuant to United States Code, title 42, section
12.17 290dd-2;

12.18 (6) information that is:

12.19 (i) maintained by an entity that meets the definition of health care provider under Code
12.20 of Federal Regulations, title 45, section 160.103, to the extent that the entity maintains the
12.21 information in the manner required of covered entities with respect to protected health
12.22 information for purposes of the Health Insurance Portability and Accountability Act of
12.23 1996, Public Law 104-191, and related regulations;

12.24 (ii) included in a limited data set, as described under Code of Federal Regulations, title
12.25 45, part 164.514(e), to the extent that the information is used, disclosed, and maintained in
12.26 the manner specified by that part;

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

12.29 (iv) originated from, or intermingled with, information described in clause (9) and that
12.30 a licensed residential mortgage originator, as defined under section 58.02, subdivision 19,
12.31 or residential mortgage servicer, as defined under section 58.02, subdivision 20, collects,

13.1 processes, uses, or maintains in the same manner as required under the laws and regulations
13.2 specified in clause (9);

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

13.5 (8) an activity involving the collection, maintenance, disclosure, sale, communication,
13.6 or use of any personal data bearing on a consumer's credit worthiness, credit standing, credit
13.7 capacity, character, general reputation, personal characteristics, or mode of living by a
13.8 consumer reporting agency, as defined in United States Code, title 15, section 1681a(f), by
13.9 a furnisher of information, as set forth in United States Code, title 15, section 1681s-2, who
13.10 provides information for use in a consumer report, as defined in United States Code, title
13.11 15, section 1681a(d), and by a user of a consumer report, as set forth in United States Code,
13.12 title 15, section 1681b, except that information is only excluded under this paragraph to the
13.13 extent that the activity involving the collection, maintenance, disclosure, sale, communication,
13.14 or use of the information by the agency, furnisher, or user is subject to regulation under the
13.15 federal Fair Credit Reporting Act, United States Code, title 15, sections 1681 to 1681x, and
13.16 the information is not collected, maintained, used, communicated, disclosed, or sold except
13.17 as authorized by the Fair Credit Reporting Act;

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

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

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

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

13.30 (13) data collected or maintained:

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

- 14.1 (ii) as the emergency contact information of an individual under item (i) if used solely
14.2 for emergency contact purposes; or
- 14.3 (iii) that is necessary for the business to retain to administer benefits for another individual
14.4 relating to the individual under item (i) if used solely for the purposes of administering those
14.5 benefits;
- 14.6 (14) personal data collected, processed, sold, or disclosed pursuant to the Minnesota
14.7 Insurance Fair Information Reporting Act in sections 72A.49 to 72A.505;
- 14.8 (15) data collected, processed, sold, or disclosed as part of a payment-only credit, check,
14.9 or cash transaction where no data about consumers, as defined in section 325O.02, are
14.10 retained;
- 14.11 (16) a state or federally chartered bank or credit union, or an affiliate or subsidiary that
14.12 is principally engaged in financial activities, as described in United States Code, title 12,
14.13 section 1843(k);
- 14.14 (17) information that originates from, or is intermingled so as to be indistinguishable
14.15 from, information described in clause (8) and that a person licensed under chapter 56 collects,
14.16 processes, uses, or maintains in the same manner as is required under the laws and regulations
14.17 specified in clause (8);
- 14.18 (18) an insurance company, as defined in section 60A.02, subdivision 4, an insurance
14.19 producer, as defined in section 60K.31, subdivision 6, a third-party administrator of
14.20 self-insurance, or an affiliate or subsidiary of any entity identified in this clause that is
14.21 principally engaged in financial activities, as described in United States Code, title 12,
14.22 section 1843(k), except that this clause does not apply to a person that, alone or in
14.23 combination with another person, establishes and maintains a self-insurance program that
14.24 does not otherwise engage in the business of entering into policies of insurance;
- 14.25 (19) a small business, as defined by the United States Small Business Administration
14.26 under Code of Federal Regulations, title 13, part 121, except that a small business identified
14.27 in this clause is subject to section 325O.075;
- 14.28 (20) a nonprofit organization that is established to detect and prevent fraudulent acts in
14.29 connection with insurance; and
- 14.30 (21) an air carrier subject to the federal Airline Deregulation Act, Public Law 95-504,
14.31 only to the extent that an air carrier collects personal data related to prices, routes, or services
14.32 and only to the extent that the provisions of the Airline Deregulation Act preempt the
14.33 requirements of this chapter.

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

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

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

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

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

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

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

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

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

(d) Taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security

16.1 appropriate to the risk and establish a clear allocation of the responsibilities between the
16.2 controller and the processor to implement the technical and organizational measures.

16.3 (e) Processing by a processor shall be governed by a contract between the controller and
16.4 the processor that is binding on both parties and that sets out the processing instructions to
16.5 which the processor is bound, including the nature and purpose of the processing, the type
16.6 of personal data subject to the processing, the duration of the processing, and the obligations
16.7 and rights of both parties. The contract shall include the requirements imposed by this
16.8 paragraph, paragraphs (c) and (d), as well as the following requirements:

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

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

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

16.23 (f) In no event shall any contract relieve a controller or a processor from the liabilities
16.24 imposed on a controller or processor by virtue of the controller's or processor's roles in the
16.25 processing relationship under this chapter.

16.26 (g) Determining whether a person is acting as a controller or processor with respect to
16.27 a specific processing of data is a fact-based determination that depends upon the context in
16.28 which personal data are to be processed. A person that is not limited in the person's processing
16.29 of personal data pursuant to a controller's instructions, or that fails to adhere to a controller's
16.30 instructions, is a controller and not a processor with respect to a specific processing of data.
16.31 A processor that continues to adhere to a controller's instructions with respect to a specific
16.32 processing of personal data remains a processor. If a processor begins, alone or jointly with
16.33 others, determining the purposes and means of the processing of personal data, the processor
16.34 is a controller with respect to the processing.

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

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

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

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

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

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

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

(g) If a consumer's personal data is profiled in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer, the consumer has the right to question the result of the profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future. The consumer has the right to review the consumer's personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

(h) A consumer has a right to obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data. If the controller does not maintain

the information in a format specific to the consumer, a list of specific third parties to whom the controller has disclosed any consumers' personal data may be provided instead.

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

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

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

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

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

(1) not unfairly disadvantage another controller;

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

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

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

19.1 (5) enable the controller to accurately determine whether the consumer is a Minnesota
19.2 resident and whether the consumer has made a legitimate request to opt out of any sale of
19.3 the consumer's personal data or targeted advertising. For purposes of this paragraph, the
19.4 use of an Internet protocol address to estimate the consumer's location is sufficient to
19.5 determine the consumer's residence.

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

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

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

19.17 Subd. 4. **Controller response to consumer requests.** (a) Except as provided in this
19.18 chapter, a controller must comply with a request to exercise the rights pursuant to subdivision
19.19 1.

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

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

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

19.29 (e) A controller must inform a consumer of any action taken on a request under
19.30 subdivision 1 without undue delay and in any event within 45 days of receipt of the request.
19.31 That period may be extended once by 45 additional days where reasonably necessary, taking
19.32 into account the complexity and number of the requests. The controller must inform the

20.1 consumer of any extension within 45 days of receipt of the request, together with the reasons
20.2 for the delay.

20.3 (f) If a controller does not take action on a consumer's request, the controller must inform
20.4 the consumer without undue delay and at the latest within 45 days of receipt of the request
20.5 of the reasons for not taking action and instructions for how to appeal the decision with the
20.6 controller as described in subdivision 3.

20.7 (g) Information provided under this section must be provided by the controller free of
20.8 charge, up to twice annually to the consumer. Where requests from a consumer are manifestly
20.9 unfounded or excessive, in particular because of the repetitive character of the requests, the
20.10 controller may either charge a reasonable fee to cover the administrative costs of complying
20.11 with the request, or refuse to act on the request. The controller bears the burden of
20.12 demonstrating the manifestly unfounded or excessive character of the request.

20.13 (h) A controller is not required to comply with a request to exercise any of the rights
20.14 under subdivision 1, paragraphs (b) to (h), if the controller is unable to authenticate the
20.15 request using commercially reasonable efforts. In such cases, the controller may request
20.16 the provision of additional information reasonably necessary to authenticate the request. A
20.17 controller is not required to authenticate an opt-out request, but a controller may deny an
20.18 opt-out request if the controller has a good faith, reasonable, and documented belief that
20.19 the request is fraudulent. If a controller denies an opt-out request because the controller
20.20 believes a request is fraudulent, the controller must notify the person who made the request
20.21 that the request was denied due to the controller's belief that the request was fraudulent and
20.22 state the controller's basis for that belief.

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

20.26 (1) Social Security number;

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

20.28 (3) financial account number;

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

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

20.31 (6) biometric data.

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

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

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

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

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

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

21.18 (c) Within 45 days of receipt of an appeal, a controller must inform the consumer of any
21.19 action taken or not taken in response to the appeal, along with a written explanation of the
21.20 reasons in support thereof. That period may be extended by 60 additional days where
21.21 reasonably necessary, taking into account the complexity and number of the requests serving
21.22 as the basis for the appeal. The controller must inform the consumer of any extension within
21.23 45 days of receipt of the appeal, together with the reasons for the delay.

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

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

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

(1) reidentify deidentified data;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

23.19 (b) If a controller sells personal data to third parties, processes personal data for targeted
23.20 advertising, or engages in profiling in furtherance of decisions that produce legal effects
23.21 concerning a consumer or similarly significant effects concerning a consumer, the controller
23.22 must disclose the processing in the privacy notice and provide access to a clear and
23.23 conspicuous method outside the privacy notice for a consumer to opt out of the sale,
23.24 processing, or profiling in furtherance of decisions that produce legal effects concerning a
23.25 consumer or similarly significant effects concerning a consumer. This method may include
23.26 but is not limited to an internet hyperlink clearly labeled "Your Opt-Out Rights" or "Your
23.27 Privacy Rights" that directly effectuates the opt-out request or takes consumers to a web
23.28 page where the consumer can make the opt-out request.

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) A controller may not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This subdivision does not: (1) require a controller to provide a good or service that requires the personal data of a consumer that the controller does not collect or maintain; or (2) prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or

services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

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

(b) unless:

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

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

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

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

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

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

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

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

(a) A controller must document and maintain a description of the policies and procedures the controller has adopted to comply with this chapter. The description must include, where applicable:

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

- 27.1 (2) a description of the controller's data privacy policies and procedures which reflect
27.2 the requirements in section 325O.07, and any policies and procedures designed to:
- 27.3 (i) reflect the requirements of this chapter in the design of the controller's systems;
27.4 (ii) identify and provide personal data to a consumer as required by this chapter;
27.5 (iii) establish, implement, and maintain reasonable administrative, technical, and physical
27.6 data security practices to protect the confidentiality, integrity, and accessibility of personal
27.7 data, including the maintenance of an inventory of the data that must be managed to exercise
27.8 the responsibilities under this item;
- 27.9 (iv) limit the collection of personal data to what is adequate, relevant, and reasonably
27.10 necessary in relation to the purposes for which the data are processed;
- 27.11 (v) prevent the retention of personal data that is no longer relevant and reasonably
27.12 necessary in relation to the purposes for which the data were collected and processed, unless
27.13 retention of the data is otherwise required by law or permitted under section 325O.09; and
- 27.14 (vi) identify and remediate violations of this chapter.
- 27.15 (b) A controller must conduct and document a data privacy and protection assessment
27.16 for each of the following processing activities involving personal data:
- 27.17 (1) the processing of personal data for purposes of targeted advertising;
27.18 (2) the sale of personal data;
27.19 (3) the processing of sensitive data;
27.20 (4) any processing activities involving personal data that present a heightened risk of
27.21 harm to consumers; and
- 27.22 (5) the processing of personal data for purposes of profiling, where the profiling presents
27.23 a reasonably foreseeable risk of:
- 27.24 (i) unfair or deceptive treatment of, or disparate impact on, consumers;
27.25 (ii) financial, physical, or reputational injury to consumers;
27.26 (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or
27.27 concerns, of consumers, where the intrusion would be offensive to a reasonable person; or
27.28 (iv) other substantial injury to consumers.

28.1 (c) A data privacy and protection assessment must take into account the type of personal
28.2 data to be processed by the controller, including the extent to which the personal data are
28.3 sensitive data, and the context in which the personal data are to be processed.

28.4 (d) A data privacy and protection assessment must identify and weigh the benefits that
28.5 may flow directly and indirectly from the processing to the controller, consumer, other
28.6 stakeholders, and the public against the potential risks to the rights of the consumer associated
28.7 with the processing, as mitigated by safeguards that can be employed by the controller to
28.8 reduce the potential risks. The use of deidentified data and the reasonable expectations of
28.9 consumers, as well as the context of the processing and the relationship between the controller
28.10 and the consumer whose personal data will be processed, must be factored into this
28.11 assessment by the controller.

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

28.14 (f) As part of a civil investigative demand, the attorney general may request, in writing,
28.15 that a controller disclose any data privacy and protection assessment that is relevant to an
28.16 investigation conducted by the attorney general. The controller must make a data privacy
28.17 and protection assessment available to the attorney general upon a request made under this
28.18 paragraph. The attorney general may evaluate the data privacy and protection assessments
28.19 for compliance with this chapter. Data privacy and protection assessments are classified as
28.20 nonpublic data, as defined by section 13.02, subdivision 9. The disclosure of a data privacy
28.21 and protection assessment pursuant to a request from the attorney general under this
28.22 paragraph does not constitute a waiver of the attorney-client privilege or work product
28.23 protection with respect to the assessment and any information contained in the assessment.

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

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

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

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

- 29.1 (1) comply with federal, state, or local laws, rules, or regulations, including but not
29.2 limited to data retention requirements in state or federal law notwithstanding a consumer's
29.3 request to delete personal data;
- 29.4 (2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or
29.5 summons by federal, state, local, or other governmental authorities;
- 29.6 (3) cooperate with law enforcement agencies concerning conduct or activity that the
29.7 controller or processor reasonably and in good faith believes may violate federal, state, or
29.8 local laws, rules, or regulations;
- 29.9 (4) investigate, establish, exercise, prepare for, or defend legal claims;
- 29.10 (5) provide a product or service specifically requested by a consumer, perform a contract
29.11 to which the consumer is a party, including fulfilling the terms of a written warranty, or
29.12 take steps at the request of the consumer prior to entering into a contract;
- 29.13 (6) take immediate steps to protect an interest that is essential for the life or physical
29.14 safety of the consumer or of another natural person, and where the processing cannot be
29.15 manifestly based on another legal basis;
- 29.16 (7) prevent, detect, protect against, or respond to security incidents, identity theft, fraud,
29.17 harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity
29.18 or security of systems; or investigate, report, or prosecute those responsible for any such
29.19 action;
- 29.20 (8) assist another controller, processor, or third party with any of the obligations under
29.21 this paragraph;
- 29.22 (9) engage in public or peer-reviewed scientific, historical, or statistical research in the
29.23 public interest that adheres to all other applicable ethics and privacy laws and is approved,
29.24 monitored, and governed by an institutional review board, human subjects research ethics
29.25 review board, or a similar independent oversight entity which has determined that:
- 29.26 (i) the research is likely to provide substantial benefits that do not exclusively accrue to
29.27 the controller;
- 29.28 (ii) the expected benefits of the research outweigh the privacy risks; and
- 29.29 (iii) the controller has implemented reasonable safeguards to mitigate privacy risks
29.30 associated with research, including any risks associated with reidentification; or
- 29.31 (10) process personal data for the benefit of the public in the areas of public health,
29.32 community health, or population health, but only to the extent that the processing is:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) In the event that a controller or processor violates this chapter, the attorney general, prior to filing an enforcement action under paragraph (b), must provide the controller or processor with a warning letter identifying the specific provisions of this chapter the attorney general alleges have been or are being violated. If, after 30 days of issuance of the warning letter, the attorney general believes the controller or processor has failed to cure any alleged violation, the attorney general may bring an enforcement action under paragraph (b). This paragraph expires January 31, 2026.

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

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

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

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

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

(b) If any provision of this chapter or this chapter's application to any person or circumstance is held invalid, the remainder of this chapter or the application of the provision to other persons or circumstances is not affected.

Sec. 14. **EFFECTIVE DATE.**

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

ARTICLE 3
COMMERCE POLICY

Section 1. Minnesota Statutes 2022, section 45.0135, subdivision 7, is amended to read:

Subd. 7. **Assessment.** Each insurer authorized to sell insurance in the state of Minnesota, including surplus lines carriers, and having Minnesota earned premium the previous calendar year shall remit an assessment to the commissioner for deposit in the insurance fraud prevention account on or before June 1 of each year. The amount of the assessment shall be based on the insurer's total assets and on the insurer's total written Minnesota premium, for the preceding fiscal year, as reported pursuant to section 60A.13. ~~The assessment is calculated to be an amount up to the following~~ Beginning with the payment due on or before June 1, 2024, the assessment amount is:

Total Assets	Assessment
	200
Less than \$100,000,000	\$ 400
	750
\$100,000,000 to \$1,000,000,000	\$ 1,500
	2,000
Over \$1,000,000,000	\$ 4,000
Minnesota Written Premium	Assessment

33.1			200
33.2	Less than \$10,000,000	\$	<u>400</u>
33.3			750
33.4	\$10,000,000 to \$100,000,000	\$	<u>1,500</u>
33.5			2,000
33.6	Over \$100,000,000	\$	<u>4,000</u>

33.7 For purposes of this subdivision, the following entities are not considered to be insurers
 33.8 authorized to sell insurance in the state of Minnesota: risk retention groups; or township
 33.9 mutuals organized under chapter 67A.

33.10 **EFFECTIVE DATE.** This section is effective the day following final enactment.

33.11 Sec. 2. **[58B.051] REGISTRATION FOR LENDERS.**

33.12 (a) Beginning January 1, 2025, a lender must register with the commissioner as a lender
 33.13 before providing services in Minnesota. A lender must not offer or make a student loan to
 33.14 a resident of Minnesota without first registering with the commissioner as provided in this
 33.15 section.

33.16 (b) A registration application must include:

33.17 (1) the lender's name;

33.18 (2) the lender's address;

33.19 (3) the names of all officers, directors, partners, and owners of controlling interests in
 33.20 the lender;

33.21 (4) the addresses of all officers, directors, partners, and owners of controlling interests
 33.22 in the lender; and

33.23 (5) any other information the commissioner requires by rule.

33.24 (c) A lender must renew the lender's registration on an annual basis and may be required
 33.25 to pay a fee at the time of renewal.

33.26 (d) The commissioner may adopt and enforce:

33.27 (1) registration procedures for lenders, which may include using the Nationwide
 33.28 Multistate Licensing System and Registry;

33.29 (2) registration fees for lenders, which may include fees for using the Nationwide
 33.30 Multistate Licensing System and Registry, to be paid directly by the lender;

(3) procedures and fees to renew a lender's registration, which may include fees for the renewed use of Nationwide Multistate Licensing System and Registry, to be paid directly by the lender; and

(4) alternate registration procedures and fees for institutions of postsecondary education that offer student loans.

Sec. 3. **[62J.96] ACCESS TO 340B DRUGS.**

Subdivision 1. **Manufacturers.** A manufacturer must not directly or indirectly restrict, prohibit, or otherwise interfere with the delivery of a covered outpatient drug to a pharmacy that is under contract with a 340B covered entity to receive and dispense covered outpatient drugs on behalf of the covered entity, unless the delivery of the drug to the pharmacy is prohibited under the 340B Drug Pricing Program.

Subd. 2. **Definitions.** (a) For purposes of this section, the following definitions apply.

(b) "340B covered entity" has the meaning provided in section 340B(a)(4) of the Public Health Service Act.

(c) "Covered outpatient drug" has the meaning provided in section 1927(k) of the Social Security Act.

(d) "Manufacturer" has the meaning provided in section 151.01, subdivision 14a.

Sec. 4. Minnesota Statutes 2022, section 62Q.73, subdivision 3, is amended to read:

Subd. 3. **Right to external review.** (a) Any enrollee or anyone acting on behalf of an enrollee who has received an adverse determination may submit a written request for an external review of the adverse determination, if applicable under section 62Q.68, subdivision 1, or 62M.06, to the commissioner of health if the request involves a health plan company regulated by that commissioner or to the commissioner of commerce if the request involves a health plan company regulated by that commissioner. Notification of the enrollee's right to external review must accompany the denial issued by the insurer. ~~The written request must be accompanied by a filing fee of \$25. The fee may be waived by the commissioner of health or commerce in cases of financial hardship and must be refunded if the adverse determination is completely reversed. No enrollee may be subject to filing fees totaling more than \$75 during a plan year for group coverage or policy year for individual coverage.~~

(b) Nothing in this section requires the commissioner of health or commerce to independently investigate an adverse determination referred for independent external review.

(c) If an enrollee requests an external review, the health plan company must participate in the external review. The cost of the external review ~~in excess of the filing fee described in paragraph (a) shall~~ must be borne by the health plan company.

(d) The enrollee must request external review within six months from the date of the adverse determination.

Sec. 5. Minnesota Statutes 2023 Supplement, section 144.197, is amended to read:

144.197 CANNABIS AND SUBSTANCE MISUSE PREVENTION AND EDUCATION PROGRAMS.

Subdivision 1. **Youth prevention and education program.** The commissioner of health, in consultation with the commissioners of human services and education and in collaboration with local health departments and Tribal health departments, shall conduct a long-term, coordinated ~~education~~ program to raise public awareness about ~~and address the top three~~ substance misuse prevention, treatment options, and recovery options. The program must address adverse health effects, as determined by the commissioner, associated with the use of cannabis flower, cannabis products, lower-potency hemp edibles, or hemp-derived consumer products by persons under age 25. In conducting this education program, the commissioner shall engage and consult with youth around the state on program content and on methods to effectively disseminate program information to youth around the state.

Subd. 2. **Prevention and education program for pregnant and breastfeeding individuals; and individuals who may become pregnant.** The commissioner of health, in consultation with the commissioners of human services and education, shall conduct a long-term, coordinated prevention program to educate focused on (1) preventing substance use by pregnant individuals, breastfeeding individuals, and individuals who may become pregnant, and (2) raising public awareness of the risks of substance use while pregnant or breastfeeding. The program must include education on the adverse health effects of prenatal exposure to cannabis flower, cannabis products, lower-potency hemp edibles, or hemp-derived consumer products and on the adverse health effects experienced by infants and children who are exposed to cannabis flower, cannabis products, lower-potency hemp edibles, or hemp-derived consumer products in breast milk, from secondhand smoke, or by ingesting cannabinoid products. This prevention and education program must also educate individuals on what constitutes a substance use disorder, signs of a substance use disorder, and treatment options for persons with a substance use disorder. The prevention and education program must also provide resources, including training resources, technical assistance, or

educational materials, to local public health home visiting programs, Tribal home visiting programs, and child welfare workers.

~~Subd. 3. **Home visiting programs.** The commissioner of health shall provide training, technical assistance, and education materials to local public health home visiting programs and Tribal home visiting programs and child welfare workers regarding the safe and unsafe use of cannabis flower, cannabis products, lower-potency hemp edibles, or hemp-derived consumer products in homes with infants and young children. Training, technical assistance, and education materials shall address substance use, the signs of a substance use disorder, treatment options for persons with a substance use disorder, the dangers of driving under the influence of cannabis flower, cannabis products, lower-potency hemp edibles, or hemp-derived consumer products, how to safely consume cannabis flower, cannabis products, lower-potency hemp edibles, or hemp-derived consumer products in homes with infants and young children, and how to prevent infants and young children from being exposed to cannabis flower, cannabis products, lower-potency hemp edibles, or hemp-derived consumer products by ingesting cannabinoid products or through secondhand smoke.~~

Subd. 4. **Local and Tribal health departments.** The commissioner of health shall distribute grants to local health departments and Tribal health departments for ~~these~~ the departments to create and disseminate educational materials on cannabis flower, cannabis products, lower-potency hemp edibles, and hemp-derived consumer products and to provide safe use and prevention training, education, technical assistance, and community engagement regarding cannabis flower, cannabis products, lower-potency hemp edibles, and hemp-derived consumer products. prevention, education, and recovery programs focusing on substance misuse prevention and treatment options. The programs must include specific cannabis-related initiatives.

Sec. 6. Minnesota Statutes 2023 Supplement, section 325E.21, subdivision 1b, is amended to read:

Subd. 1b. **Purchase or acquisition record required.** (a) Every scrap metal dealer, including an agent, employee, or representative of the dealer, shall create a permanent record written in English, using an electronic record program at the time of each purchase or acquisition of scrap metal or a motor vehicle. The record must include:

(1) a complete and accurate account or description, including the weight if customarily purchased by weight, of the scrap metal or motor vehicle purchased or acquired;

(2) the date, time, and place of the receipt of the scrap metal or motor vehicle purchased or acquired and a unique transaction identifier;

(3) a photocopy or electronic scan of the seller's proof of identification including the identification number;

(4) the amount paid and the number of the check or electronic transfer used to purchase or acquire the scrap metal or motor vehicle;

(5) the license plate number and description of the vehicle used by the person when delivering the scrap metal or motor vehicle, including the vehicle make and model, and any identifying marks on the vehicle, such as a business name, decals, or markings, if applicable;

(6) a statement signed by the seller, under penalty of perjury as provided in section 609.48, attesting that the scrap metal or motor vehicle is not stolen and is free of any liens or encumbrances and the seller has the right to sell it;

(7) a copy of the receipt, which must include at least the following information: the name and address of the dealer, the date and time the scrap metal or motor vehicle was received by the dealer, an accurate description of the scrap metal or motor vehicle, and the amount paid for the scrap metal or motor vehicle;

(8) in order to purchase or acquire a detached catalytic converter, the vehicle identification number of the car it was removed from or, as an alternative, any numbers, bar codes, stickers, or other unique markings, whether resulting from the pilot project created under subdivision 2b or some other source. The alternative number must be under a numbering system that can be immediately linked to the vehicle identification number by law enforcement; ~~and~~

(9) the identity or identifier of the employee completing the transaction; and

(10) if the seller is attempting to sell copper metal, a photocopy or electronic scan of the seller's current license to sell scrap metal copper issued by the commissioner under subdivision 2c.

(b) The record, as well as the scrap metal or motor vehicle purchased or acquired, shall at all reasonable times be open to the inspection of any properly identified law enforcement officer.

(c) Except for the purchase or acquisition of detached catalytic converters or motor vehicles, no record is required for property purchased or acquired from merchants, manufacturers, salvage pools, insurance companies, rental car companies, financial institutions, charities, dealers licensed under section 168.27, or wholesale dealers, having an established place of business, or of any goods purchased or acquired at open sale from any bankrupt stock, but a receipt as required under paragraph (a), clause (7), shall be obtained

38.1 and kept by the person, which must be shown upon demand to any properly identified law
38.2 enforcement officer.

38.3 (d) The dealer must provide a copy of the receipt required under paragraph (a), clause
38.4 (7), to the seller in every transaction.

38.5 (e) The commissioner of public safety and law enforcement agencies in the jurisdiction
38.6 where a dealer is located may conduct inspections and audits as necessary to ensure
38.7 compliance, refer violations to the city or county attorney for criminal prosecution, and
38.8 notify the registrar of motor vehicles.

38.9 (f) Except as otherwise provided in this section, a scrap metal dealer or the dealer's agent,
38.10 employee, or representative may not disclose personal information concerning a customer
38.11 without the customer's consent unless the disclosure is required by law or made in response
38.12 to a request from a law enforcement agency. A scrap metal dealer must implement reasonable
38.13 safeguards to protect the security of the personal information and prevent unauthorized
38.14 access to or disclosure of the information. For purposes of this paragraph, "personal
38.15 information" is any individually identifiable information gathered in connection with a
38.16 record under paragraph (a).

38.17 Sec. 7. Minnesota Statutes 2022, section 325E.21, is amended by adding a subdivision to
38.18 read:

38.19 Subd. 2c. **License required for scrap metal copper sale.** (a) Beginning January 1,
38.20 2025, a person is prohibited from engaging in the sale of scrap metal copper unless the
38.21 person has a valid license issued by the commissioner under this subdivision.

38.22 (b) A seller of scrap metal copper may apply to the commissioner on a form prescribed
38.23 by the commissioner. The application form must include, at a minimum:

38.24 (1) the name, permanent address, telephone number, and date of birth of the applicant;
38.25 and

38.26 (2) an acknowledgment that the applicant obtained the copper by lawful means in the
38.27 regular course of the applicant's business, trade, or authorized construction work.

38.28 (c) Each application must be accompanied by a nonrefundable fee of \$250.

38.29 (d) Within 30 days of the date an application is received, the commissioner may require
38.30 additional information or submissions from an applicant and may obtain any document or
38.31 information that is reasonably necessary to verify the information contained in the application.
38.32 Within 90 days after the date a completed application is received, the commissioner must

review the application and issue a license if the applicant is deemed qualified under this section. The commissioner may issue a license subject to restrictions or limitations. If the commissioner determines the applicant is not qualified, the commissioner must notify the applicant and must specify the reason for the denial.

(e) A person licensed to perform work pursuant to chapter 326B or issued a Section 608 Technician Certification is deemed to hold a license to sell scrap metal copper.

(f) A license issued under this subdivision is valid for one year. To renew a license, an applicant must submit a completed renewal application on a form prescribed by the commissioner and a renewal fee of \$250. The commissioner may request that a renewal applicant submit additional information to clarify any new information presented in the renewal application. A renewal application submitted after the renewal deadline must be accompanied by a nonrefundable late fee of \$500.

(g) The commissioner may deny a license renewal under this subdivision if:

(1) the commissioner determines that the applicant is in violation of or noncompliant with federal or state law; or

(2) the applicant fails to timely submit a renewal application and the information required under this subdivision.

(h) In lieu of denying a renewal application under paragraph (g), the commissioner may permit the applicant to submit to the commissioner a corrective action plan to cure or correct deficiencies.

(i) The commissioner may suspend, revoke, or place on probation a license issued under this subdivision if:

(1) the applicant engages in fraudulent activity that violates state or federal law;

(2) the commissioner receives consumer complaints that justify an action under this subdivision to protect the safety and interests of consumers;

(3) the applicant fails to pay an application license or renewal fee; or

(4) the applicant fails to comply with a requirement set forth in this subdivision.

(j) This subdivision does not apply to transfers by or to an auctioneer who is in compliance with chapter 330 and acting in the person's official role as an auctioneer to facilitate or conduct an auction of scrap metal.

(k) The commissioner must enforce this subdivision under chapter 45.

Sec. 8. Minnesota Statutes 2023 Supplement, section 342.72, is amended to read:

342.72 SUBSTANCE USE TREATMENT, RECOVERY, AND PREVENTION GRANTS.

Subdivision 1. ~~Account established;~~ **Appropriation.** A substance use treatment, recovery, and prevention grant ~~account~~ is created ~~in the special revenue fund~~. Money ~~in the account, including interest earned,~~ is appropriated to the office commissioner of health for the purposes specified in this section. ~~Of the amount transferred from the general fund to the account, the office may use up to five percent for administrative expenses.~~

~~Subd. 2. **Acceptance of gifts and grants.** Notwithstanding sections 16A.013 to 16A.016, the office may accept money contributed by individuals and may apply for grants from charitable foundations to be used for the purposes identified in this section. The money accepted under this section must be deposited in the substance use treatment, recovery, and prevention grant account created under subdivision 1.~~

Subd. 3. **Disposition of money; grants.** (a) Money ~~in the substance use treatment, recovery, and prevention grant account~~ appropriated to the commissioner of health for purposes of this section must be distributed as follows:

(1) at least 75 percent of the money is for grants for substance use disorder and mental health recovery and prevention programs. Funds must be used for recovery and prevention activities and supplies that assist individuals and families to initiate, stabilize, and maintain long-term recovery from substance use disorders and co-occurring mental health conditions. Recovery and prevention activities may include prevention education, school-linked behavioral health, school-based peer programs, peer supports, self-care and wellness, culturally specific healing, community public awareness, mutual aid networks, telephone recovery checkups, mental health warmlines, harm reduction, recovery community organization development, first episode psychosis programs, and recovery housing; and

(2) up to 25 percent of the money is for substance use disorder treatment programs as defined in chapter 245G and may be used to implement, strengthen, or expand supportive services and activities that are not covered by medical assistance under chapter 256B, MinnesotaCare under chapter 256L, or the behavioral health fund under chapter 254B. Services and activities may include adoption or expansion of evidence-based practices; competency-based training; continuing education; culturally specific and culturally responsive services; sober recreational activities; developing referral relationships; family preservation and healing; and start-up or capacity funding for programs that specialize in adolescent,

41.1 culturally specific, culturally responsive, disability-specific, co-occurring disorder, or family
41.2 treatment services.

41.3 (b) The ~~office~~ commissioner of health shall consult with the Governor's Advisory Council
41.4 on Opioids, Substance Use, and Addiction; the commissioner of human services; and ~~the~~
41.5 ~~commissioner of health~~ the Office of Cannabis Management to develop an appropriate
41.6 application process, establish grant requirements, determine what organizations are eligible
41.7 to receive grants, and establish reporting requirements for grant recipients.

41.8 Subd. 4. **Reports to the legislature.** By January 15, 2024, and each January 15 thereafter
41.9 year, the ~~office~~ commissioner of health must submit a report to the chairs and ranking
41.10 minority members of the committees of the house of representatives and the senate having
41.11 jurisdiction over health and human services policy and finance that details grants awarded
41.12 from the substance use treatment, recovery, and prevention grant account, including the
41.13 total amount awarded, total number of recipients, and geographic distribution of those
41.14 recipients.