INTRODUCTION

02/21/23 REVISOR JFK/EH 23-03726

This Document can be made available in alternative formats upon request

State of Minnesota

HOUSE OF REPRESENTATIVES

NINETY-THIRD SESSION

H. F. No. 2309

03/01/2023 Authored by Elkins, Bahner, Noor and Feist
The bill was read for the first time and referred to the Committee on Commerce Finance and Policy

A bill for an act

relating to consumer data privacy; giving various rights to consumers regarding personal data; placing obligations on certain businesses regarding consumer data; providing for enforcement by the attorney general; proposing coding for new law in Minnesota Statutes, chapter 13; proposing coding for new law as Minnesota Statutes, chapter 325O.

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

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

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

MN
pg 1

STATE OF CONNECTICUT

Substitute Senate Bill No. 6

Public Act No. 22-15

CT
pg 1

AN ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective July 1, 2023*) As used in this section and sections 2 to 11, inclusive, of this act, unless the context otherwise requires:

Intro / MN, CT / 1

SENATE BILL 21-190

BY SENATOR(S) Rodriguez and Lundeen, Bridges, Buckner, Coleman, Cooke, Danielson, Donovan, Fenberg, Gardner, Ginal, Gonzales, Hansen, Hisey, Holbert, Jaquez Lewis, Kirkmeyer, Kolker, Lee, Liston, Moreno, Pettersen, Priola, Rankin, Scott, Simpson, Sonnenberg, Story, Winter, Woodward, Garcia;
also REPRESENTATIVE(S) Duran and Carver, Bernett, Bird, Cutter, Exum, Gonzales-Gutierrez, Gray, Herod, Jodeh, Lynch, McCluskie, McCormick, Mullica, Ricks, Snyder, Titone, Valdez A., Woodrow.

CD
pg 1

CONCERNING ADDITIONAL PROTECTION OF DATA RELATING TO PERSONAL PRIVACY.

Be it enacted by the General Assembly of the State of Colorado:

SECTION 1. In Colorado Revised Statutes, **add** part 13 to article 1 of title 6 as follows:

PART 13
COLORADO PRIVACY ACT

6-1-1301. Short title. THE SHORT TITLE OF THIS PART 13 IS THE "COLORADO PRIVACY ACT".

Capital letters or bold & italic numbers indicate new material added to existing law; dashes through words or numbers indicate deletions from existing law and such material is not part of the act.

INTRO/ col 1

6-1-1302. Legislative declaration. (1) THE GENERAL ASSEMBLY HEREBY:

(a) FINDS THAT:

(I) THE PEOPLE OF COLORADO REGARD THEIR PRIVACY AS A FUNDAMENTAL RIGHT AND AN ESSENTIAL ELEMENT OF THEIR INDIVIDUAL FREEDOM;

(II) COLORADO'S CONSTITUTION EXPLICITLY PROVIDES THE RIGHT TO PRIVACY UNDER SECTION 7 OF ARTICLE II, AND FUNDAMENTAL PRIVACY RIGHTS HAVE LONG BEEN, AND CONTINUE TO BE, INTEGRAL TO PROTECTING COLORADANS AND TO SAFEGUARDING OUR DEMOCRATIC REPUBLIC;

CO (cont'd)

(III) ONGOING ADVANCES IN TECHNOLOGY HAVE PRODUCED EXPONENTIAL GROWTH IN THE VOLUME AND VARIETY OF PERSONAL DATA BEING GENERATED, COLLECTED, STORED, AND ANALYZED AND THESE ADVANCES PRESENT BOTH PROMISE AND POTENTIAL PERIL;

(IV) THE ABILITY TO HARNESS AND USE DATA IN POSITIVE WAYS IS DRIVING INNOVATION AND BRINGS BENEFICIAL TECHNOLOGIES TO SOCIETY, BUT IT HAS ALSO CREATED RISKS TO PRIVACY AND FREEDOM; AND

(V) THE UNAUTHORIZED DISCLOSURE OF PERSONAL INFORMATION AND LOSS OF PRIVACY CAN HAVE DEVASTATING IMPACTS RANGING FROM FINANCIAL FRAUD, IDENTITY THEFT, AND UNNECESSARY COSTS IN PERSONAL TIME AND FINANCES TO DESTRUCTION OF PROPERTY, HARASSMENT, REPUTATIONAL DAMAGE, EMOTIONAL DISTRESS, AND PHYSICAL HARM;

(b) DETERMINES THAT:

(I) TECHNOLOGICAL INNOVATION AND NEW USES OF DATA CAN HELP SOLVE SOCIETAL PROBLEMS AND IMPROVE LIVES, AND IT IS POSSIBLE TO BUILD A WORLD WHERE TECHNOLOGICAL INNOVATION AND PRIVACY CAN COEXIST; AND

(II) STATES ACROSS THE UNITED STATES ARE LOOKING TO THIS PART 13 AND SIMILAR MODELS TO ENACT STATE-BASED DATA PRIVACY REQUIREMENTS AND TO EXERCISE THE LEADERSHIP THAT IS LACKING AT THE

Intro | CO|2

NATIONAL LEVEL; AND

(c) DECLARES THAT:

(I) BY ENACTING THIS PART 13, COLORADO WILL BE AMONG THE STATES THAT EMPOWER CONSUMERS TO PROTECT THEIR PRIVACY AND REQUIRE COMPANIES TO BE RESPONSIBLE CUSTODIANS OF DATA AS THEY CONTINUE TO INNOVATE;

(II) THIS PART 13 ADDRESSES ISSUES OF STATEWIDE CONCERN AND:

CO cont'd

(A) PROVIDES CONSUMERS THE RIGHT TO ACCESS, CORRECT, AND DELETE PERSONAL DATA AND THE RIGHT TO OPT OUT NOT ONLY OF THE SALE OF PERSONAL DATA BUT ALSO OF THE COLLECTION AND USE OF PERSONAL DATA;

(B) IMPOSES AN AFFIRMATIVE OBLIGATION UPON COMPANIES TO SAFEGUARD PERSONAL DATA; TO PROVIDE CLEAR, UNDERSTANDABLE, AND TRANSPARENT INFORMATION TO CONSUMERS ABOUT HOW THEIR PERSONAL DATA ARE USED; AND TO STRENGTHEN COMPLIANCE AND ACCOUNTABILITY BY REQUIRING DATA PROTECTION ASSESSMENTS IN THE COLLECTION AND USE OF PERSONAL DATA; AND

(C) EMPOWERS THE ATTORNEY GENERAL AND DISTRICT ATTORNEYS TO ACCESS AND EVALUATE A COMPANY'S DATA PROTECTION ASSESSMENTS, TO IMPOSE PENALTIES WHERE VIOLATIONS OCCUR, AND TO PREVENT FUTURE VIOLATIONS.

DATA PRACTICES

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.

MN only

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.

1/MN/1

DEFINITIONS

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

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

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

MN

(1) "Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity. For the purposes of this subdivision, "control" or "controlled" means (A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company, (B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or (C) the power to exercise controlling influence over the management of a company.

CT

6-1-1303. Definitions. AS USED IN THIS PART 13, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(1) "AFFILIATE" MEANS A LEGAL ENTITY THAT CONTROLS, IS CONTROLLED BY, OR IS UNDER COMMON CONTROL WITH ANOTHER LEGAL ENTITY. AS USED IN THIS SUBSECTION (1), "CONTROL" MEANS:

(a) OWNERSHIP OF, CONTROL OF, OR POWER TO VOTE TWENTY-FIVE PERCENT OR MORE OF THE OUTSTANDING SHARES OF ANY CLASS OF VOTING SECURITY OF THE ENTITY, DIRECTLY OR INDIRECTLY, OR ACTING THROUGH ONE OR MORE OTHER PERSONS;

CO

(b) CONTROL IN ANY MANNER OVER THE ELECTION OF A MAJORITY OF THE DIRECTORS, TRUSTEES, OR GENERAL PARTNERS OF THE ENTITY OR OF INDIVIDUALS EXERCISING SIMILAR FUNCTIONS; OR

(c) THE POWER TO EXERCISE, DIRECTLY OR INDIRECTLY, A CONTROLLING INFLUENCE OVER THE MANAGEMENT OR POLICIES OF THE ENTITY AS DETERMINED BY THE APPLICABLE PRUDENTIAL REGULATOR, AS THAT TERM IS DEFINED IN 12 U.S.C. SEC. 5481 (24), IF ANY.

3/ MN CT CO/1

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

MN

(2) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 4 of this act is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

CT

(2) "AUTHENTICATE" MEANS TO USE REASONABLE MEANS TO DETERMINE THAT A REQUEST TO EXERCISE ANY OF THE RIGHTS IN SECTION 6-1-1306 (1) IS BEING MADE BY OR ON BEHALF OF THE CONSUMER WHO IS ENTITLED TO EXERCISE THE RIGHTS.

CO

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

MN

(1) a digital or physical photograph;

(2) an audio or video recording; or

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

(3) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

CT

3/ MN CT CO/2

(4) "Business associate" has the same meaning as provided in HIPAA. CT

(3) "BUSINESS ASSOCIATE" HAS THE MEANING ESTABLISHED IN 45 CFR 160.103. CO

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

(5) "Child" has the same meaning as provided in COPPA. CT

(4) "CHILD" MEANS AN INDIVIDUAL UNDER THIRTEEN YEARS OF AGE. CO

3/MN CT CO/3

(f) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of personal data relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, consent cannot be obtained through a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice. A consumer may revoke consent previously given, consistent with this chapter.

MN

(6) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include (A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, (B) hovering over, muting, pausing or closing a given piece of content, or (C) agreement obtained through the use of dark patterns.

CT

(5) "CONSENT" MEANS A CLEAR, AFFIRMATIVE ACT SIGNIFYING A CONSUMER'S FREELY GIVEN, SPECIFIC, INFORMED, AND UNAMBIGUOUS AGREEMENT, SUCH AS BY A WRITTEN STATEMENT, INCLUDING BY ELECTRONIC MEANS, OR OTHER CLEAR, AFFIRMATIVE ACTION BY WHICH THE CONSUMER SIGNIFIES AGREEMENT TO THE PROCESSING OF PERSONAL DATA. THE FOLLOWING DOES NOT CONSTITUTE CONSENT:

CO

(a) ACCEPTANCE OF A GENERAL OR BROAD TERMS OF USE OR SIMILAR DOCUMENT THAT CONTAINS DESCRIPTIONS OF PERSONAL DATA PROCESSING ALONG WITH OTHER, UNRELATED INFORMATION;

(b) HOVERING OVER, MUTING, PAUSING, OR CLOSING A GIVEN PIECE OF CONTENT; AND

(c) AGREEMENT OBTAINED THROUGH DARK PATTERNS.

3 / MN CT CO 4

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

MN

(7) "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

CT

(6) "CONSUMER":

(a) MEANS AN INDIVIDUAL WHO IS A COLORADO RESIDENT ACTING ONLY IN AN INDIVIDUAL OR HOUSEHOLD CONTEXT; AND

(b) DOES NOT INCLUDE AN INDIVIDUAL ACTING IN A COMMERCIAL OR EMPLOYMENT CONTEXT, AS A JOB APPLICANT, OR AS A BENEFICIARY OF SOMEONE ACTING IN AN EMPLOYMENT CONTEXT.

CO

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

MN

(8) "Controller" means an individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data.

CT

(7) "CONTROLLER" MEANS A PERSON THAT, ALONE OR JOINTLY WITH OTHERS, DETERMINES THE PURPOSES FOR AND MEANS OF PROCESSING PERSONAL DATA.

CO

3/MN CT CO/5

(9) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

CT

---

(10) "Covered entity" has the same meaning as provided in HIPAA.

CT

(8) "COVERED ENTITY" HAS THE MEANING ESTABLISHED IN 45 CFR 160.103.

CO

---

(11) "Dark pattern" (A) means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and (B) includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

CT

(9) "DARK PATTERN" MEANS A USER INTERFACE DESIGNED OR MANIPULATED WITH THE SUBSTANTIAL EFFECT OF SUBVERTING OR IMPAIRING USER AUTONOMY, DECISION-MAKING, OR CHOICE.

CO

3/MN CT CO/6

(i) "Decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer" means decisions that result in the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

MN

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

CT

(10) "DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER" MEANS A DECISION THAT RESULTS IN THE PROVISION OR DENIAL OF FINANCIAL OR LENDING SERVICES, HOUSING, INSURANCE, EDUCATION ENROLLMENT OR OPPORTUNITY, CRIMINAL JUSTICE, EMPLOYMENT OPPORTUNITIES, HEALTH-CARE SERVICES, OR ACCESS TO ESSENTIAL GOODS OR SERVICES.

CO

3/MN CT CO/7

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

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

MN

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

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

(13) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data (A) takes reasonable measures to ensure that such data cannot be associated with an individual, (B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

CT

(11) "DE-IDENTIFIED DATA" MEANS DATA THAT CANNOT REASONABLY BE USED TO INFER INFORMATION ABOUT, OR OTHERWISE BE LINKED TO, AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL, OR A DEVICE LINKED TO SUCH AN INDIVIDUAL, IF THE CONTROLLER THAT POSSESSES THE DATA:

CO

(a) TAKES REASONABLE MEASURES TO ENSURE THAT THE DATA CANNOT BE ASSOCIATED WITH AN INDIVIDUAL;

(b) PUBLICLY COMMITS TO MAINTAIN AND USE THE DATA ONLY IN A DE-IDENTIFIED FASHION AND NOT ATTEMPT TO RE-IDENTIFY THE DATA; AND

(c) CONTRACTUALLY OBLIGATES ANY RECIPIENTS OF THE INFORMATION TO COMPLY WITH THE REQUIREMENTS OF THIS SUBSECTION (11).

3 / MN CT CO 18

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

MN

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

MN

---

(12) "HEALTH-CARE FACILITY" MEANS ANY ENTITY THAT IS LICENSED, CERTIFIED, OR OTHERWISE AUTHORIZED OR PERMITTED BY LAW TO ADMINISTER MEDICAL TREATMENT IN THIS STATE.

CO

3/MN CT CO/9

MN
CT

(13) "HEALTH-CARE INFORMATION" MEANS INDIVIDUALLY IDENTIFIABLE INFORMATION RELATING TO THE PAST, PRESENT, OR FUTURE HEALTH STATUS OF AN INDIVIDUAL.

CO

(14) "HEALTH-CARE PROVIDER" MEANS A PERSON LICENSED, CERTIFIED, OR REGISTERED IN THIS STATE TO PRACTICE MEDICINE, PHARMACY, CHIROPRACTIC, NURSING, PHYSICAL THERAPY, PODIATRY, DENTISTRY, OPTOMETRY, OCCUPATIONAL THERAPY, OR OTHER HEALING ARTS UNDER TITLE 12.

MN

(14) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

CT

(15) "HIPAA" MEANS THE FEDERAL "HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996", AS AMENDED, 42 U.S.C. SECS. 1320d TO 1320d-9.

CO

3/MN CT CO/10

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

MN

(15) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

CT

(16) "IDENTIFIED OR IDENTIFIABLE INDIVIDUAL" MEANS AN INDIVIDUAL WHO CAN BE READILY IDENTIFIED, DIRECTLY OR INDIRECTLY, IN PARTICULAR BY REFERENCE TO AN IDENTIFIER SUCH AS A NAME, AN IDENTIFICATION NUMBER, SPECIFIC GEOLOCATION DATA, OR AN ONLINE IDENTIFIER.

CO

(n) "Known child" means a person under circumstances where a controller has actual knowledge of, or willfully disregards, that the person is under 18 years of age.

MN

---

(16) "Institution of higher education" means any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

CT

---

(17) "Nonprofit organization" means any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time.

CT

3/MN CT CO/11

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

MN

(18) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

CT

(17) "PERSONAL DATA":

(a) MEANS INFORMATION THAT IS LINKED OR REASONABLY LINKABLE TO AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL; AND

(b) DOES NOT INCLUDE DE-IDENTIFIED DATA OR PUBLICLY AVAILABLE INFORMATION. AS USED IN THIS SUBSECTION (17)(b), "PUBLICLY AVAILABLE INFORMATION" MEANS INFORMATION THAT IS LAWFULLY MADE AVAILABLE FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS AND INFORMATION THAT A CONTROLLER HAS A REASONABLE BASIS TO BELIEVE THE CONSUMER HAS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC.

CO

3 / MN CT CO / 12

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

(20) "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data. CT

(18) "PROCESS" OR "PROCESSING" MEANS THE COLLECTION, USE, SALE, STORAGE, DISCLOSURE, ANALYSIS, DELETION, OR MODIFICATION OF PERSONAL DATA AND INCLUDES THE ACTIONS OF A CONTROLLER DIRECTING A PROCESSOR TO PROCESS PERSONAL DATA. CO

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

(21) "Processor" means an individual who, or legal entity that, processes personal data on behalf of a controller. CT

(19) "PROCESSOR" MEANS A PERSON THAT PROCESSES PERSONAL DATA ON BEHALF OF A CONTROLLER. CO

3/MN CT CO/13

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

MN

(22) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

CT

(20) "PROFILING" MEANS ANY FORM OF AUTOMATED PROCESSING OF PERSONAL DATA TO EVALUATE, ANALYZE, OR PREDICT PERSONAL ASPECTS CONCERNING AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL'S ECONOMIC SITUATION, HEALTH, PERSONAL PREFERENCES, INTERESTS, RELIABILITY, BEHAVIOR, LOCATION, OR MOVEMENTS.

CO

3/MN CT CO/14

MN

(23) "Protected health information" has the same meaning as provided in HIPAA.

CT

(21) "PROTECTED HEALTH INFORMATION" HAS THE MEANING ESTABLISHED IN 45 CFR 160.103.

CO

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

MN

(24) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

CT

(22) "PSEUDONYMOUS DATA" MEANS PERSONAL DATA THAT CAN NO LONGER BE ATTRIBUTED TO A SPECIFIC INDIVIDUAL WITHOUT THE USE OF ADDITIONAL INFORMATION IF THE ADDITIONAL INFORMATION IS KEPT SEPARATELY AND IS SUBJECT TO TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THAT THE PERSONAL DATA ARE NOT ATTRIBUTED TO A SPECIFIC INDIVIDUAL.

CO

---

(25) "Publicly available information" means information that (A) is lawfully made available through federal, state or municipal government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

CT

3/MN CT CO/15

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

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

(2) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer;

MN

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

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

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

(26) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include (A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller, (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer, (C) the disclosure or transfer of personal data to an affiliate of the controller, (D) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party, (E) the disclosure of personal data that the consumer (i) intentionally made available to the general public via a channel of mass media, and (ii) did not restrict to a specific audience, or (F) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller's assets.

CT

(cont)

(23) (a) "SALE", "SELL", OR "SOLD" MEANS THE EXCHANGE OF PERSONAL DATA FOR MONETARY OR OTHER VALUABLE CONSIDERATION BY A CONTROLLER TO A THIRD PARTY.

(b) "SALE", "SELL", OR "SOLD" DOES NOT INCLUDE THE FOLLOWING:

(I) THE DISCLOSURE OF PERSONAL DATA TO A PROCESSOR THAT PROCESSES THE PERSONAL DATA ON BEHALF OF A CONTROLLER;

(II) THE DISCLOSURE OF PERSONAL DATA TO A THIRD PARTY FOR PURPOSES OF PROVIDING A PRODUCT OR SERVICE REQUESTED BY THE CONSUMER; CO

(III) THE DISCLOSURE OR TRANSFER OF PERSONAL DATA TO AN AFFILIATE OF THE CONTROLLER;

(IV) THE DISCLOSURE OR TRANSFER TO A THIRD PARTY OF PERSONAL DATA AS AN ASSET THAT IS PART OF A PROPOSED OR ACTUAL MERGER, ACQUISITION, BANKRUPTCY, OR OTHER TRANSACTION IN WHICH THE THIRD PARTY ASSUMES CONTROL OF ALL OR PART OF THE CONTROLLER'S ASSETS; OR

(V) THE DISCLOSURE OF PERSONAL DATA:

(A) THAT A CONSUMER DIRECTS THE CONTROLLER TO DISCLOSE OR INTENTIONALLY DISCLOSES BY USING THE CONTROLLER TO INTERACT WITH A THIRD PARTY; OR

(B) INTENTIONALLY MADE AVAILABLE BY A CONSUMER TO THE GENERAL PUBLIC VIA A CHANNEL OF MASS MEDIA.

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

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

(2) the processing of biometric data or genetic information;

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

(4) specific geolocation data.

MN

(27) "Sensitive data" means personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (C) personal data collected from a known child, or (D) precise geolocation data.

CT

(24) "SENSITIVE DATA" MEANS:

(a) PERSONAL DATA REVEALING RACIAL OR ETHNIC ORIGIN, RELIGIOUS BELIEFS, A MENTAL OR PHYSICAL HEALTH CONDITION OR DIAGNOSIS, SEX LIFE OR SEXUAL ORIENTATION, OR CITIZENSHIP OR CITIZENSHIP STATUS;

CO

(b) GENETIC OR BIOMETRIC DATA THAT MAY BE PROCESSED FOR THE PURPOSE OF UNIQUELY IDENTIFYING AN INDIVIDUAL; OR

(c) PERSONAL DATA FROM A KNOWN CHILD.

3/MN CT CO/17

(v) "Specific geolocation data" means information derived from technology, including but not limited to global positioning system level latitude, longitude, or altitude coordinates; cellular phone system coordinates; internet protocol device addresses; or other mechanisms that can be used to identify a specific street or postal address associated with the consumer. Specific geolocation data excludes the content of communications and the contents of databases containing name and address information which are accessible to the public as authorized by law.

MN

Sec. 3. 4

(19) "Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

CT

CO ?

3 IMN CT CO / 1B

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

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

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

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

MN

(28) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include (A) advertisements based on activities within a controller's own Internet web sites or online applications, (B) advertisements based on the context of a consumer's current search query, visit to an Internet web site or online application, (C) advertisements directed to a consumer in response to the consumer's request for information or feedback, or (D) processing personal data solely to measure or report advertising frequency, performance or reach.

CT

(25) "TARGETED ADVERTISING":

(a) MEANS DISPLAYING TO A CONSUMER AN ADVERTISEMENT THAT IS SELECTED BASED ON PERSONAL DATA OBTAINED OR INFERRED OVER TIME FROM THE CONSUMER'S ACTIVITIES ACROSS NONAFFILIATED WEBSITES, APPLICATIONS, OR ONLINE SERVICES TO PREDICT CONSUMER PREFERENCES OR INTERESTS; AND

(b) DOES NOT INCLUDE:

CO

(I) ADVERTISING TO A CONSUMER IN RESPONSE TO THE CONSUMER'S REQUEST FOR INFORMATION OR FEEDBACK;

(II) ADVERTISEMENTS BASED ON ACTIVITIES WITHIN A CONTROLLER'S OWN WEBSITES OR ONLINE APPLICATIONS;

(III) ADVERTISEMENTS BASED ON THE CONTEXT OF A CONSUMER'S CURRENT SEARCH QUERY, VISIT TO A WEBSITE, OR ONLINE APPLICATION; OR

(IV) PROCESSING PERSONAL DATA SOLELY FOR MEASURING OR REPORTING ADVERTISING PERFORMANCE, REACH, OR FREQUENCY.

3 / MN CT CO / 19

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

MN

(29) "Third party" means an individual or legal entity, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the processor or the controller.

CT

(26) "THIRD PARTY" MEANS A PERSON, PUBLIC AUTHORITY, AGENCY, OR BODY OTHER THAN A CONSUMER, CONTROLLER, PROCESSOR, OR AFFILIATE OF THE PROCESSOR OR THE CONTROLLER.

CO

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

MN

(30) "Trade secret" has the same meaning as provided in section 35-51 of the general statutes.

CT

CO?

3 IMN CT CO/20

SCOPE

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

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

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

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

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

MN

pg 5

Sec. 2. (NEW) (*Effective July 1, 2023*) The provisions of sections 1 to 11, inclusive, of this act apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year: (1) Controlled or processed the personal data of not less than one hundred thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) controlled or processed the personal data of not less than twenty-five thousand consumers and derived more than twenty-five per cent of their gross revenue from the sale of personal data.

CT

pg 7

6-1-1304. Applicability of part. (1) EXCEPT AS SPECIFIED IN SUBSECTION (2) OF THIS SECTION, THIS PART 13 APPLIES TO A CONTROLLER THAT:

(a) CONDUCTS BUSINESS IN COLORADO OR PRODUCES OR DELIVERS COMMERCIAL PRODUCTS OR SERVICES THAT ARE INTENTIONALLY TARGETED TO RESIDENTS OF COLORADO; AND

CO

(b) SATISFIES ONE OR BOTH OF THE FOLLOWING THRESHOLDS:

(I) CONTROLS OR PROCESSES THE PERSONAL DATA OF ONE HUNDRED THOUSAND CONSUMERS OR MORE DURING A CALENDAR YEAR; OR

pg 9

(II) DERIVES REVENUE OR RECEIVES A DISCOUNT ON THE PRICE OF GOODS OR SERVICES FROM THE SALE OF PERSONAL DATA AND PROCESSES OR CONTROLS THE PERSONAL DATA OF TWENTY-FIVE THOUSAND CONSUMERS OR MORE.

4.1 / MN CT CO / I

Exclusions

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

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

(2) a federally recognized Indian tribe;

(3) information that meets the definition of:

MN p95

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

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

(cont'd)

4.2/MN 11

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

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

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

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

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

MN

pg 6

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

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

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

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

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

(7) an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in United States Code, title 15, section 1681a(f), by a furnisher of information, as set forth in United States Code, title 15, section 1681s-2, who provides information for use in a consumer report, as defined in United States Code, title 15, section 1681a(d), and by a user of a consumer report, as set forth in United States Code,

4.2 / MN 12

title 15, section 1681b, except that information is only excluded under this paragraph to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the federal Fair Credit Reporting Act, United States Code, title 15, sections 1681 to 1681x, and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act;

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

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

MN

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

p97

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

(12) data collected or maintained:

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

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

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

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

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

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

MN pg 8

4.2 | MN 14

Sec. 3. (NEW) (*Effective July 1, 2023*) (a) The provisions of sections 1 to 11, inclusive, of this act do not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; (2) nonprofit organization; (3) institution of higher education; (4) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; (5) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; or (6) covered entity or business associate, as defined in 45 CFR 160.103.

(b) The following information and data is exempt from the provisions of sections 1 to 11, inclusive, of this act: (1) Protected health information under HIPAA; (2) patient-identifying information for purposes of 42 USC 290dd-2; (3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46; (4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501,

CT
pg 7

4.2/CT 11

that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law; (6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.; (7) patient safety work product for purposes of section 19a-127o of the general statutes and the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time; (8) information derived from any of the health care related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; (9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time; (10) information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities; (11) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time; (13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time; (14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time; (15) data processed or maintained (A) in the course of an individual applying to, employed by

CT

pg 8

4,2 | CT | 2

or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role, (B) as the emergency contact information of an individual under sections 1 to 11, inclusive, of this act used for emergency contact purposes, or (C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits; and (16) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Airline Deregulation Act, 49 USC 40101 et seq., as amended from time to time, by an air carrier subject to said act, to the extent sections 1 to 11, inclusive, of this act are preempted by the Airline Deregulation Act, 49 USC 41713, as amended from time to time.

CT

AG

(c) Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to sections 1 to 11, inclusive, of this act.

(2) THIS PART 13 DOES NOT APPLY TO:

(a) PROTECTED HEALTH INFORMATION THAT IS COLLECTED, STORED, AND PROCESSED BY A COVERED ENTITY OR ITS BUSINESS ASSOCIATES;

(b) HEALTH-CARE INFORMATION THAT IS GOVERNED BY PART 8 OF ARTICLE 1 OF TITLE 25 SOLELY FOR THE PURPOSE OF ACCESS TO MEDICAL RECORDS;

CO
pg 9

(c) PATIENT IDENTIFYING INFORMATION, AS DEFINED IN 42 CFR 2.11, THAT ARE GOVERNED BY AND COLLECTED AND PROCESSED PURSUANT TO 42 CFR 2, ESTABLISHED PURSUANT TO 42 U.S.C. SEC. 290dd-2;

(d) IDENTIFIABLE PRIVATE INFORMATION, AS DEFINED IN 45 CFR 46.102, FOR PURPOSES OF THE FEDERAL POLICY FOR THE PROTECTION OF

(cont'd)

4.2/co/1

HUMAN SUBJECTS PURSUANT TO 45 CFR 46; IDENTIFIABLE PRIVATE INFORMATION THAT IS COLLECTED AS PART OF HUMAN SUBJECTS RESEARCH PURSUANT TO THE ICH E6 GOOD CLINICAL PRACTICE GUIDELINE ISSUED BY THE INTERNATIONAL COUNCIL FOR HARMONISATION OF TECHNICAL REQUIREMENTS FOR PHARMACEUTICALS FOR HUMAN USE OR THE PROTECTION OF HUMAN SUBJECTS UNDER 21 CFR 50 AND 56; OR PERSONAL DATA USED OR SHARED IN RESEARCH CONDUCTED IN ACCORDANCE WITH ONE OR MORE OF THE CATEGORIES SET FORTH IN THIS SUBSECTION (2)(d);

(e) INFORMATION AND DOCUMENTS CREATED BY A COVERED ENTITY FOR PURPOSES OF COMPLYING WITH HIPAA AND ITS IMPLEMENTING REGULATIONS;

CO
pg 10

(f) PATIENT SAFETY WORK PRODUCT, AS DEFINED IN 42 CFR 3.20, THAT IS CREATED FOR PURPOSES OF PATIENT SAFETY IMPROVEMENT PURSUANT TO 42 CFR 3, ESTABLISHED PURSUANT TO 42 U.S.C. SECS. 299b-21 TO 299b-26;

(g) INFORMATION THAT IS:

(I) DE-IDENTIFIED IN ACCORDANCE WITH THE REQUIREMENTS FOR DE-IDENTIFICATION SET FORTH IN 45 CFR 164; AND

(II) DERIVED FROM ANY OF THE HEALTH-CARE-RELATED INFORMATION DESCRIBED IN THIS SECTION.

(h) INFORMATION MAINTAINED IN THE SAME MANNER AS INFORMATION UNDER SUBSECTIONS (2)(a) TO (2)(g) OF THIS SECTION BY:

(I) A COVERED ENTITY OR BUSINESS ASSOCIATE;

(II) A HEALTH-CARE FACILITY OR HEALTH-CARE PROVIDER; OR

(III) A PROGRAM OF A QUALIFIED SERVICE ORGANIZATION AS DEFINED IN 42 CFR 2.11;

(i) (I) EXCEPT AS PROVIDED IN SUBSECTION (2)(i)(II) OF THIS SECTION, AN ACTIVITY INVOLVING THE COLLECTION, MAINTENANCE, DISCLOSURE, SALE, COMMUNICATION, OR USE OF ANY PERSONAL DATA BEARING ON A CONSUMER'S CREDITWORTHINESS, CREDIT STANDING, CREDIT

4/21/CO/2

CAPACITY, CHARACTER, GENERAL REPUTATION, PERSONAL CHARACTERISTICS, OR MODE OF LIVING BY:

(A) A CONSUMER REPORTING AGENCY AS DEFINED IN 15 U.S.C. SEC. 1681a (f);

(B) A FURNISHER OF INFORMATION AS SET FORTH IN 15 U.S.C. SEC. 1681s-2 THAT PROVIDES INFORMATION FOR USE IN A CONSUMER REPORT, AS DEFINED IN 15 U.S.C. SEC. 1681a (d); OR

(C) A USER OF A CONSUMER REPORT AS SET FORTH IN 15 U.S.C. SEC. 1681b.

(II) THIS SUBSECTION (2)(i) APPLIES ONLY TO THE EXTENT THAT THE ACTIVITY IS REGULATED BY THE FEDERAL "FAIR CREDIT REPORTING ACT", 15 U.S.C. SEC. 1681 ET SEQ., AS AMENDED, AND THE PERSONAL DATA ARE NOT COLLECTED, MAINTAINED, DISCLOSED, SOLD, COMMUNICATED, OR USED EXCEPT AS AUTHORIZED BY THE FEDERAL "FAIR CREDIT REPORTING ACT", AS AMENDED.

CO

pa 11

(j) PERSONAL DATA:

(I) COLLECTED AND MAINTAINED FOR PURPOSES OF ARTICLE 22 OF TITLE 10;

(II) COLLECTED, PROCESSED, SOLD, OR DISCLOSED PURSUANT TO THE FEDERAL "GRAMM-LEACH-BLILEY ACT", 15 U.S.C. SEC. 6801 ET SEQ., AS AMENDED, AND IMPLEMENTING REGULATIONS, IF THE COLLECTION, PROCESSING, SALE, OR DISCLOSURE IS IN COMPLIANCE WITH THAT LAW;

(III) COLLECTED, PROCESSED, SOLD, OR DISCLOSED PURSUANT TO THE FEDERAL "DRIVER'S PRIVACY PROTECTION ACT OF 1994", 18 U.S.C. SEC. 2721 ET SEQ., AS AMENDED, IF THE COLLECTION, PROCESSING, SALE, OR DISCLOSURE IS REGULATED BY THAT LAW, INCLUDING IMPLEMENTING RULES, REGULATIONS, OR EXEMPTIONS;

(IV) REGULATED BY THE FEDERAL "CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998", 15 U.S.C. SECS. 6501 TO 6506, AS AMENDED, IF COLLECTED, PROCESSED, AND MAINTAINED IN COMPLIANCE WITH THAT LAW; OR

4.2 / CO / 3

(V) REGULATED BY THE FEDERAL "FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT OF 1974", 20 U.S.C. SEC. 1232g ET SEQ., AS AMENDED, AND ITS IMPLEMENTING REGULATIONS;

(k) DATA MAINTAINED FOR EMPLOYMENT RECORDS PURPOSES;

(l) AN AIR CARRIER AS DEFINED IN AND REGULATED UNDER 49 U.S.C. SEC. 40101 ET SEQ., AS AMENDED, AND 49 U.S.C. SEC. 41713, AS AMENDED;

(m) A NATIONAL SECURITIES ASSOCIATION REGISTERED PURSUANT TO THE FEDERAL "SECURITIES EXCHANGE ACT OF 1934", 15 U.S.C. SEC. 78o-3, AS AMENDED, OR IMPLEMENTING REGULATIONS;

CO

(n) CUSTOMER DATA MAINTAINED BY A PUBLIC UTILITY AS DEFINED IN SECTION 40-1-103 (1)(a)(I) OR AN AUTHORITY AS DEFINED IN SECTION 43-4-503 (1), IF THE DATA ARE NOT COLLECTED, MAINTAINED, DISCLOSED, SOLD, COMMUNICATED, OR USED EXCEPT AS AUTHORIZED BY STATE AND FEDERAL LAW;

pg 12

(o) DATA MAINTAINED BY A STATE INSTITUTION OF HIGHER EDUCATION, AS DEFINED IN SECTION 23-18-102 (10), THE STATE, THE JUDICIAL DEPARTMENT OF THE STATE, OR A COUNTY, CITY AND COUNTY, OR MUNICIPALITY IF THE DATA IS COLLECTED, MAINTAINED, DISCLOSED, COMMUNICATED, AND USED AS AUTHORIZED BY STATE AND FEDERAL LAW FOR NONCOMMERCIAL PURPOSES. THIS SUBSECTION (2)(o) DOES NOT EFFECT ANY OTHER EXEMPTION AVAILABLE UNDER THIS PART 13.

(p) INFORMATION USED AND DISCLOSED IN COMPLIANCE WITH 45 CFR 164.512; OR

(q) A FINANCIAL INSTITUTION OR AN AFFILIATE OF A FINANCIAL INSTITUTION AS DEFINED BY AND THAT IS SUBJECT TO THE FEDERAL "GRAMM-LEACH-BLILEY ACT", 15 U.S.C. SEC. 6801 ET SEQ., AS AMENDED, AND IMPLEMENTING REGULATIONS, INCLUDING REGULATION P, 12 CFR 1016.

4.2/co/3

Responsibilities According to Role

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

(a) Controllers and processors are responsible for meeting their 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 its obligations under this chapter. Such assistance 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) Notwithstanding the instructions of the controller, a processor shall:

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

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

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

(e) Processing by a processor shall be governed by a contract between the controller and the processor that is binding on both parties and that sets out the processing instructions to which the processor is bound, including the nature and purpose of the processing, the type

of personal data subject to the processing, the duration of the processing, and the obligations and rights of both parties. In addition, the contract shall include the requirements imposed by this paragraph, paragraphs (c) and (d), as well as the following requirements:

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

(2) the processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this chapter; and

(3) the processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. Alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit of the processor's policies and technical and organizational measures in support of the obligations under this chapter. The auditor must use an appropriate and accepted control standard or framework and audit procedure for such audits as applicable, and shall provide a report of such audit to the controller upon request.

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

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

Sec. 7. (NEW) (*Effective July 1, 2023*) (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under sections 1 to 11, inclusive, of this act. Such assistance shall include: (1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests; (2) taking into account the nature of processing and the information available to the processor, by assisting 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 security, as defined in section 36a-701b of the general statutes, of the system of the processor, in order to meet the controller's obligations; and (3) providing necessary information to

CT
pg 16

16

SICT11

enable the controller to conduct and document data protection assessments.

(b) 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 personal data is subject to a duty of confidentiality with respect to the data; (2) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 1 to 11, inclusive, of this act; (4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and (5) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 1 to 11, inclusive, of this act, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

CT
P917

(c) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing

5/CT/2

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under section 11 of this act.

CT
pg 18

6-1-1305. Responsibility according to role. (1) CONTROLLERS AND PROCESSORS SHALL MEET THEIR RESPECTIVE OBLIGATIONS ESTABLISHED UNDER THIS PART 13.

(2) PROCESSORS SHALL ADHERE TO THE INSTRUCTIONS OF THE CONTROLLER AND ASSIST THE CONTROLLER TO MEET ITS OBLIGATIONS UNDER THIS PART 13. TAKING INTO ACCOUNT THE NATURE OF PROCESSING AND THE INFORMATION AVAILABLE TO THE PROCESSOR, THE PROCESSOR SHALL ASSIST THE CONTROLLER BY:

(a) TAKING 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 6-1-1306;

CO
pg 15

(b) HELPING TO MEET 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 6-1-716; AND

(c) PROVIDING INFORMATION TO THE CONTROLLER NECESSARY TO ENABLE THE CONTROLLER TO CONDUCT AND DOCUMENT ANY DATA PROTECTION ASSESSMENTS REQUIRED BY SECTION 6-1-1309. THE CONTROLLER AND PROCESSOR ARE EACH RESPONSIBLE FOR ONLY THE MEASURES ALLOCATED TO THEM.

(3) NOTWITHSTANDING THE INSTRUCTIONS OF THE CONTROLLER, A PROCESSOR SHALL:

(a) ENSURE THAT EACH PERSON PROCESSING THE PERSONAL DATA IS SUBJECT TO A DUTY OF CONFIDENTIALITY WITH RESPECT TO THE DATA; AND

(b) ENGAGE A SUBCONTRACTOR ONLY AFTER PROVIDING THE

5 | CO | 1

CONTROLLER WITH AN OPPORTUNITY TO OBJECT AND PURSUANT TO A WRITTEN CONTRACT IN ACCORDANCE WITH SUBSECTION (5) OF THIS SECTION THAT REQUIRES THE SUBCONTRACTOR TO MEET THE OBLIGATIONS OF THE PROCESSOR WITH RESPECT TO THE PERSONAL DATA.

(4) TAKING INTO ACCOUNT THE CONTEXT OF PROCESSING, THE CONTROLLER AND THE PROCESSOR SHALL IMPLEMENT APPROPRIATE TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE A LEVEL OF SECURITY APPROPRIATE TO THE RISK AND ESTABLISH A CLEAR ALLOCATION OF THE RESPONSIBILITIES BETWEEN THEM TO IMPLEMENT THE MEASURES.

(5) PROCESSING BY A PROCESSOR MUST BE GOVERNED BY A CONTRACT BETWEEN THE CONTROLLER AND THE PROCESSOR THAT IS BINDING ON BOTH PARTIES AND THAT SETS OUT:

CO
pg 16

(a) THE PROCESSING INSTRUCTIONS TO WHICH THE PROCESSOR IS BOUND, INCLUDING THE NATURE AND PURPOSE OF THE PROCESSING;

(b) THE TYPE OF PERSONAL DATA SUBJECT TO THE PROCESSING, AND THE DURATION OF THE PROCESSING;

(c) THE REQUIREMENTS IMPOSED BY THIS SUBSECTION (5) AND SUBSECTIONS (3) AND (4) OF THIS SECTION; AND

(d) THE FOLLOWING REQUIREMENTS:

(I) AT THE CHOICE OF THE CONTROLLER, THE PROCESSOR SHALL DELETE OR RETURN ALL PERSONAL DATA TO THE CONTROLLER AS REQUESTED AT THE END OF THE PROVISION OF SERVICES, UNLESS RETENTION OF THE PERSONAL DATA IS REQUIRED BY LAW;

(II) (A) THE PROCESSOR SHALL MAKE AVAILABLE TO THE CONTROLLER ALL INFORMATION NECESSARY TO DEMONSTRATE COMPLIANCE WITH THE OBLIGATIONS IN THIS PART 13; AND

(B) THE PROCESSOR SHALL ALLOW FOR, AND CONTRIBUTE TO, REASONABLE AUDITS AND INSPECTIONS BY THE CONTROLLER OR THE CONTROLLER'S DESIGNATED AUDITOR. ALTERNATIVELY, THE PROCESSOR MAY, WITH THE CONTROLLER'S CONSENT, ARRANGE FOR A QUALIFIED AND INDEPENDENT AUDITOR TO CONDUCT, AT LEAST ANNUALLY AND AT THE

5/CO/2

PROCESSOR'S EXPENSE, AN AUDIT OF THE PROCESSOR'S POLICIES AND TECHNICAL AND ORGANIZATIONAL MEASURES IN SUPPORT OF THE OBLIGATIONS UNDER THIS PART 13 USING AN APPROPRIATE AND ACCEPTED CONTROL STANDARD OR FRAMEWORK AND AUDIT PROCEDURE FOR THE AUDITS AS APPLICABLE. THE PROCESSOR SHALL PROVIDE A REPORT OF THE AUDIT TO THE CONTROLLER UPON REQUEST.

(6) IN NO EVENT MAY A CONTRACT RELIEVE A CONTROLLER OR A PROCESSOR FROM THE LIABILITIES IMPOSED ON THEM BY VIRTUE OF ITS ROLE IN THE PROCESSING RELATIONSHIP AS DEFINED BY THIS PART 13.

(7) DETERMINING WHETHER A PERSON IS ACTING AS A CONTROLLER OR PROCESSOR WITH RESPECT TO A SPECIFIC PROCESSING OF DATA IS A FACT-BASED DETERMINATION THAT DEPENDS UPON THE CONTEXT IN WHICH PERSONAL DATA ARE TO BE PROCESSED. A PERSON THAT IS NOT LIMITED IN ITS PROCESSING OF PERSONAL DATA PURSUANT TO A CONTROLLER'S INSTRUCTIONS, OR THAT FAILS TO ADHERE TO THE INSTRUCTIONS, IS A CONTROLLER AND NOT A PROCESSOR WITH RESPECT TO A SPECIFIC PROCESSING OF DATA. A PROCESSOR THAT CONTINUES TO ADHERE TO A CONTROLLER'S INSTRUCTIONS WITH RESPECT TO A SPECIFIC PROCESSING OF PERSONAL DATA REMAINS A PROCESSOR. IF A PROCESSOR BEGINS, ALONE OR JOINTLY WITH OTHERS, DETERMINING THE PURPOSES AND MEANS OF THE PROCESSING OF PERSONAL DATA, IT IS A CONTROLLER WITH RESPECT TO THE PROCESSING.

CO, pg 17

(8) (a) A CONTROLLER OR PROCESSOR THAT DISCLOSES PERSONAL DATA TO ANOTHER CONTROLLER OR PROCESSOR IN COMPLIANCE WITH THIS PART 13 DOES NOT VIOLATE THIS PART 13 IF THE RECIPIENT PROCESSES THE PERSONAL DATA IN VIOLATION OF THIS PART 13, AND, 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.

(b) A CONTROLLER OR PROCESSOR RECEIVING PERSONAL DATA FROM A CONTROLLER OR PROCESSOR IN COMPLIANCE WITH THIS PART 13 AS SPECIFIED IN SUBSECTION (8)(a) OF THIS SECTION DOES NOT VIOLATE THIS PART 13 IF THE CONTROLLER OR PROCESSOR FROM WHICH IT RECEIVES THE PERSONAL DATA FAILS TO COMPLY WITH APPLICABLE OBLIGATIONS UNDER THIS PART 13.

5/co/3

BASIC CONSUMER PERSONAL DATA RIGTS

Sec. 6. **[325O.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.

MN

(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 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 such profiling and be informed of the reason that the profiling resulted in the decision, as well as the actions that 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 customer's personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

c.1 | MN | 1

Sec. 4. (NEW) (*Effective July 1, 2023*) (a) A consumer shall have the right to: (1) Confirm whether or not a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret; (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data; (3) delete personal data provided by, or obtained about, the consumer; (4) obtain a copy of the consumer's personal data processed by 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, provided such controller shall not be required to reveal any trade secret; and (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subsection (b) of section 6 of this act, or (C) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

CT

PG 9

Sec. 5. (NEW) (*Effective July 1, 2023*) A consumer may designate another person to serve as the consumer's authorized agent, and act on such consumer's behalf, to opt out of the processing of such consumer's personal data for one or more of the purposes specified in subdivision (5) of subsection (a) of section 4 of this act. The consumer may designate such 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 such consumer's intent to opt out of such 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 such consumer's behalf.

CT

PG 12

6.1 | CT | 1

6-1-1306. Consumer personal data rights - repeal.

(b) **Right of access.** A CONSUMER HAS THE RIGHT TO CONFIRM WHETHER A CONTROLLER IS PROCESSING PERSONAL DATA CONCERNING THE CONSUMER AND TO ACCESS THE CONSUMER'S PERSONAL DATA.

(c) **Right to correction.** A CONSUMER HAS THE RIGHT TO CORRECT INACCURACIES IN THE CONSUMER'S PERSONAL DATA, TAKING INTO ACCOUNT THE NATURE OF THE PERSONAL DATA AND THE PURPOSES OF THE PROCESSING OF THE CONSUMER'S PERSONAL DATA.

(d) **Right to deletion.** A CONSUMER HAS THE RIGHT TO DELETE PERSONAL DATA CONCERNING THE CONSUMER.

(e) **Right to data portability.** WHEN EXERCISING THE RIGHT TO ACCESS PERSONAL DATA PURSUANT TO SUBSECTION (1)(b) OF THIS SECTION, A CONSUMER HAS THE RIGHT TO OBTAIN THE PERSONAL DATA IN A PORTABLE AND, TO THE EXTENT TECHNICALLY FEASIBLE, READILY USABLE FORMAT THAT ALLOWS THE CONSUMER TO TRANSMIT THE DATA TO ANOTHER ENTITY WITHOUT HINDRANCE. A CONSUMER MAY EXERCISE THIS RIGHT NO MORE THAN TWO TIMES PER CALENDAR YEAR. NOTHING IN THIS SUBSECTION (1)(e) REQUIRES A CONTROLLER TO PROVIDE THE DATA TO THE CONSUMER IN A MANNER THAT WOULD DISCLOSE THE CONTROLLER'S TRADE SECRETS.

6/10/11

(a) **Right to opt out.** (I) A CONSUMER HAS THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER FOR PURPOSES OF:

(A) TARGETED ADVERTISING;

(B) THE SALE OF PERSONAL DATA; OR

(C) PROFILING IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER. CO

(II) A CONSUMER MAY AUTHORIZE ANOTHER PERSON, ACTING ON THE CONSUMER'S BEHALF, TO OPT OUT OF THE PROCESSING OF THE CONSUMER'S PERSONAL DATA FOR ONE OR MORE OF THE PURPOSES SPECIFIED IN SUBSECTION (1)(a)(I) OF THIS SECTION, INCLUDING THROUGH A TECHNOLOGY INDICATING THE CONSUMER'S INTENT TO OPT OUT SUCH AS A WEB LINK INDICATING A PREFERENCE OR BROWSER SETTING, BROWSER EXTENSION, OR GLOBAL DEVICE SETTING. A CONTROLLER SHALL COMPLY WITH AN OPT-OUT REQUEST RECEIVED FROM A PERSON AUTHORIZED BY THE CONSUMER TO ACT ON THE CONSUMER'S BEHALF IF THE CONTROLLER IS ABLE TO AUTHENTICATE, WITH COMMERCIALLY REASONABLE EFFORT, THE IDENTITY OF THE CONSUMER AND THE AUTHORIZED AGENT'S AUTHORITY TO ACT ON THE CONSUMER'S BEHALF.

(III) A CONTROLLER THAT PROCESSES PERSONAL DATA FOR pg 18

6.1/co/2

PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA SHALL PROVIDE A CLEAR AND CONSPICUOUS METHOD TO EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER PURSUANT TO SUBSECTION (1)(a)(I) OF THIS SECTION. THE CONTROLLER SHALL PROVIDE THE OPT-OUT METHOD CLEARLY AND CONSPICUOUSLY IN ANY PRIVACY NOTICE REQUIRED TO BE PROVIDED TO CONSUMERS UNDER THIS PART 13, AND IN A CLEAR, CONSPICUOUS, AND READILY ACCESSIBLE LOCATION OUTSIDE THE PRIVACY NOTICE.

(IV) (A) A CONTROLLER THAT PROCESSES PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA MAY ALLOW CONSUMERS TO EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO SUBSECTIONS (1)(a)(I)(A) AND (1)(a)(I)(B) OF THIS SECTION BY CONTROLLERS THROUGH A USER-SELECTED UNIVERSAL OPT-OUT MECHANISM THAT MEETS THE TECHNICAL SPECIFICATIONS ESTABLISHED BY THE ATTORNEY GENERAL PURSUANT TO SECTION 6-1-1313. THIS SUBSECTION (1)(a)(IV)(A) IS REPEALED, EFFECTIVE JULY 1, 2024.

CO

pg 19

(B) EFFECTIVE JULY 1, 2024, A CONTROLLER THAT PROCESSES PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA SHALL ALLOW CONSUMERS TO EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO SUBSECTIONS (1)(a)(I)(A) AND (1)(a)(I)(B) OF THIS SECTION BY CONTROLLERS THROUGH A USER-SELECTED UNIVERSAL OPT-OUT MECHANISM THAT MEETS THE TECHNICAL SPECIFICATIONS ESTABLISHED BY THE ATTORNEY GENERAL PURSUANT TO SECTION 6-1-1313.

(C) NOTWITHSTANDING A CONSUMER'S DECISION TO EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA THROUGH A UNIVERSAL OPT-OUT MECHANISM PURSUANT TO SUBSECTION (1)(a)(IV)(B) OF THIS SECTION, A CONTROLLER MAY ENABLE THE CONSUMER TO CONSENT, THROUGH A WEB PAGE, APPLICATION, OR A SIMILAR METHOD, TO THE PROCESSING OF THE CONSUMER'S PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA, AND THE CONSENT TAKES PRECEDENCE OVER ANY CHOICE REFLECTED THROUGH THE UNIVERSAL OPT-OUT MECHANISM. BEFORE OBTAINING A CONSUMER'S CONSENT TO PROCESS PERSONAL DATA FOR PURPOSES OF TARGETED

6.1 CO 13

ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO THIS SUBSECTION (1)(a)(IV)(C), A CONTROLLER SHALL PROVIDE THE CONSUMER WITH A CLEAR AND CONSPICUOUS NOTICE INFORMING THE CONSUMER ABOUT THE CHOICES AVAILABLE UNDER THIS SECTION, DESCRIBING THE CATEGORIES OF PERSONAL DATA TO BE PROCESSED AND THE PURPOSES FOR WHICH THEY WILL BE PROCESSED, AND EXPLAINING HOW AND WHERE THE CONSUMER MAY WITHDRAW CONSENT. THE WEB PAGE, APPLICATION, OR OTHER MEANS BY WHICH A CONTROLLER OBTAINS A CONSUMER'S CONSENT TO PROCESS PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA MUST ALSO ALLOW THE CONSUMER TO REVOKE THE CONSENT AS EASILY AS IT IS AFFIRMATIVELY PROVIDED.

CO
pg 20

6.1 CO 14

Excercising Consomer Data Rights

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.

MN

Sec. 6. 10

(b) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 5 of this act to exercise the rights of such consumer to opt out of the processing of such consumer's personal data for purposes of subdivision (5) of subsection (a) of this section on behalf of the consumer. In the case of processing personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

CT

pg 10

6.2 / MN CT / 1

6-1-1306. Consumer personal data rights - repeal. (1) CONSUMERS MAY EXERCISE THE FOLLOWING RIGHTS BY SUBMITTING A REQUEST USING THE METHODS SPECIFIED BY THE CONTROLLER IN THE PRIVACY NOTICE REQUIRED UNDER SECTION 6-1-1308 (1)(a). THE METHOD MUST TAKE INTO ACCOUNT THE WAYS IN WHICH CONSUMERS NORMALLY INTERACT WITH THE CONTROLLER, THE NEED FOR SECURE AND RELIABLE COMMUNICATION RELATING TO THE REQUEST, AND THE ABILITY OF THE CONTROLLER TO AUTHENTICATE THE IDENTITY OF THE CONSUMER MAKING THE REQUEST. CONTROLLERS SHALL NOT REQUIRE A CONSUMER TO CREATE A NEW ACCOUNT IN ORDER TO EXERCISE CONSUMER RIGHTS PURSUANT TO THIS SECTION BUT MAY REQUIRE A CONSUMER TO USE AN EXISTING ACCOUNT. A CONSUMER MAY SUBMIT A REQUEST AT ANY TIME TO A CONTROLLER SPECIFYING WHICH OF THE FOLLOWING RIGHTS THE CONSUMER WISHES TO EXERCISE:

CO

pg 18

6.2/CO/1

Universal Opt-Out

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 such personal data through an opt-out preference signal sent, with such consumer's consent, by a platform, technology, or mechanism to the controller indicating such consumer's intent to opt out of any such 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

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

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

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

A controller shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. Any such means shall include:

(A) (i) Providing a clear and conspicuous link on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and

(ii) Not later than January 1, 2025, allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall:

CT

(I) Not unfairly disadvantage another controller;

(II) Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of such consumer's personal data pursuant to sections 1 to 11, inclusive, of this act;

(III) Be consumer-friendly and easy to use by the average consumer;

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

(V) Enable the controller to accurately determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising.

6.3/CT/1

(B) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent in accordance with the provisions of subparagraph (A) of this subdivision conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts or club card program, the controller shall comply with such consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program.

CT
pg 16

(2) If a controller responds to consumer opt-out requests received pursuant to subparagraph (A) of subdivision (1) of this subsection by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subsection (b) of this section for the retention, use, sale or sharing of the consumer's personal data.

6-1-1313. Rules - opt-out mechanism. (1) THE ATTORNEY GENERAL MAY PROMULGATE RULES FOR THE PURPOSE OF CARRYING OUT THIS PART 13.

(2) BY JULY 1, 2023, THE ATTORNEY GENERAL SHALL ADOPT RULES THAT DETAIL THE TECHNICAL SPECIFICATIONS FOR ONE OR MORE UNIVERSAL OPT-OUT MECHANISMS THAT CLEARLY COMMUNICATE A CONSUMER'S AFFIRMATIVE, FREELY GIVEN, AND UNAMBIGUOUS CHOICE TO OPT OUT OF THE PROCESSING OF PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO SECTION 6-1-1306 (1)(a)(I)(A) OR (1)(a)(I)(B). THE ATTORNEY GENERAL MAY UPDATE THE RULES THAT DETAIL THE TECHNICAL SPECIFICATIONS FOR THE MECHANISMS FROM TIME TO TIME TO REFLECT THE MEANS BY WHICH CONSUMERS INTERACT WITH CONTROLLERS. THE RULES MUST:

(a) NOT PERMIT THE MANUFACTURER OF A PLATFORM, BROWSER, DEVICE, OR ANY OTHER PRODUCT OFFERING A UNIVERSAL OPT-OUT MECHANISM TO UNFAIRLY DISADVANTAGE ANOTHER CONTROLLER; CO 28

(b) REQUIRE CONTROLLERS TO INFORM CONSUMERS ABOUT THE OPT-OUT CHOICES AVAILABLE UNDER SECTION 6-1-1306 (1)(a)(I);

(c) NOT ADOPT A MECHANISM THAT IS A DEFAULT SETTING, BUT RATHER CLEARLY REPRESENTS THE CONSUMER'S AFFIRMATIVE, FREELY GIVEN, AND UNAMBIGUOUS CHOICE TO OPT OUT OF THE PROCESSING OF PERSONAL DATA PURSUANT TO SECTION 6-1-1306 (1)(a)(I)(A) OR (1)(a)(I)(B);

(d) ADOPT A MECHANISM THAT IS CONSUMER-FRIENDLY, CLEARLY DESCRIBED, AND EASY TO USE BY THE AVERAGE CONSUMER;

(e) ADOPT A MECHANISM THAT IS AS CONSISTENT AS POSSIBLE WITH ANY OTHER SIMILAR MECHANISM REQUIRED BY LAW OR REGULATION IN THE UNITED STATES; AND

(f) PERMIT THE CONTROLLER TO ACCURATELY AUTHENTICATE THE CONSUMER AS A RESIDENT OF THIS STATE AND DETERMINE THAT THE MECHANISM REPRESENTS A LEGITIMATE REQUEST TO OPT OUT OF THE PROCESSING OF PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO SECTION 6-1-1306 (1)(a)(I)(A) OR (1)(a)(I)(B). CO 29

(3) BY JANUARY 1, 2025, THE ATTORNEY GENERAL MAY ADOPT RULES THAT GOVERN THE PROCESS OF ISSUING OPINION LETTERS AND INTERPRETIVE GUIDANCE TO DEVELOP AN OPERATIONAL FRAMEWORK FOR BUSINESS THAT INCLUDES A GOOD FAITH RELIANCE DEFENSE OF AN ACTION THAT MAY OTHERWISE CONSTITUTE A VIOLATION OF THIS PART 13. THE RULES MUST BECOME EFFECTIVE BY JULY 1, 2025.

Controller Response to Consumer Request

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

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

6.4 / MN / 1

(1) Social Security number;

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

(3) financial account number;

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

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

(6) biometric data.

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

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

(d) A controller must comply with a request to exercise the right in subdivision 1, paragraph (f), as soon as feasibly possible, but no later than 15 days of receipt of the request.

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

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

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

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

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

(c) Except as otherwise provided in sections 1 to 11, inclusive, of this act, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

(1) A controller shall respond to the consumer without undue delay, but not later than forty-five days after receipt of the request. The controller may extend the response period by forty-five additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial forty-five-day response period and of the reason for the extension.

CT

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay,

6.4 /CT/ 1

but not later than forty-five days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any twelve-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of this section using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights. A controller shall not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision

6.4/CT/2

(3) of subsection (a) of this section by (A) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose pursuant to the provisions of sections 1 to 11, inclusive, of this act, or (B) opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of sections 1 to 11, inclusive, of this act.

CT

pg 12

6.4/CT/3

(2) **Responding to consumer requests.** (a) A CONTROLLER SHALL INFORM A CONSUMER OF ANY ACTION TAKEN ON A REQUEST UNDER SUBSECTION (1) OF THIS SECTION WITHOUT UNDUE DELAY AND, IN ANY EVENT, WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE REQUEST. THE CONTROLLER MAY EXTEND THE FORTY-FIVE-DAY PERIOD BY FORTY-FIVE ADDITIONAL DAYS WHERE REASONABLY NECESSARY, TAKING INTO ACCOUNT

CO
pg 20

6.4 | co11

THE COMPLEXITY AND NUMBER OF THE REQUESTS. THE CONTROLLER SHALL INFORM THE CONSUMER OF AN EXTENSION WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE REQUEST, TOGETHER WITH THE REASONS FOR THE DELAY.

(b) IF A CONTROLLER DOES NOT TAKE ACTION ON THE REQUEST OF A CONSUMER, THE CONTROLLER SHALL INFORM THE CONSUMER, WITHOUT UNDUE DELAY AND, AT THE LATEST, WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE REQUEST, OF THE REASONS FOR NOT TAKING ACTION AND INSTRUCTIONS FOR HOW TO APPEAL THE DECISION WITH THE CONTROLLER AS DESCRIBED IN SUBSECTION (3) OF THIS SECTION.

(c) UPON REQUEST, A CONTROLLER SHALL PROVIDE TO THE CONSUMER THE INFORMATION SPECIFIED IN THIS SECTION FREE OF CHARGE; EXCEPT THAT, FOR A SECOND OR SUBSEQUENT REQUEST WITHIN A TWELVE-MONTH PERIOD, THE CONTROLLER MAY CHARGE AN AMOUNT CALCULATED IN THE MANNER SPECIFIED IN SECTION 24-72-205 (5)(a).

(d) A CONTROLLER IS NOT REQUIRED TO COMPLY WITH A REQUEST TO EXERCISE ANY OF THE RIGHTS UNDER SUBSECTION (1) OF THIS SECTION IF THE CONTROLLER IS UNABLE TO AUTHENTICATE THE REQUEST USING COMMERCIALLY REASONABLE EFFORTS, IN WHICH CASE THE CONTROLLER MAY REQUEST THE PROVISION OF ADDITIONAL INFORMATION REASONABLY NECESSARY TO AUTHENTICATE THE REQUEST. Co pg 21

(3) (a) A CONTROLLER SHALL ESTABLISH AN INTERNAL PROCESS WHEREBY CONSUMERS MAY APPEAL A REFUSAL TO TAKE ACTION ON A REQUEST TO EXERCISE ANY OF THE RIGHTS UNDER SUBSECTION (1) OF THIS SECTION WITHIN A REASONABLE PERIOD AFTER THE CONSUMER'S RECEIPT OF THE NOTICE SENT BY THE CONTROLLER UNDER SUBSECTION (2)(b) OF THIS SECTION. THE APPEAL PROCESS MUST BE CONSPICUOUSLY AVAILABLE AND AS EASY TO USE AS THE PROCESS FOR SUBMITTING A REQUEST UNDER THIS SECTION.

(b) WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF AN APPEAL, A CONTROLLER SHALL INFORM THE CONSUMER OF ANY ACTION TAKEN OR NOT TAKEN IN RESPONSE TO THE APPEAL, ALONG WITH A WRITTEN EXPLANATION OF THE REASONS IN SUPPORT OF THE RESPONSE. THE CONTROLLER MAY EXTEND THE FORTY-FIVE-DAY PERIOD BY SIXTY ADDITIONAL DAYS WHERE REASONABLY NECESSARY, TAKING INTO ACCOUNT THE COMPLEXITY AND NUMBER OF REQUESTS SERVING AS THE BASIS FOR THE APPEAL. THE

6.4 / co / 2

CONTROLLER SHALL INFORM THE CONSUMER OF AN EXTENSION WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE APPEAL, TOGETHER WITH THE REASONS FOR THE DELAY.

CO
pg 22

(c) THE CONTROLLER SHALL INFORM THE CONSUMER OF THE CONSUMER'S ABILITY TO CONTACT THE ATTORNEY GENERAL IF THE CONSUMER HAS CONCERNS ABOUT THE RESULT OF THE APPEAL.

6.4 / CO / 3

Appeal Process

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

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

(c) Within 30 days of receipt of an appeal, a controller must inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support thereof. That period may be extended by 60 additional days where reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller must inform the consumer of any such extension within 30 days of receipt of the appeal, together with the reasons for the delay. The controller must also provide the consumer with an e-mail address or other online mechanism through which the consumer may submit the appeal, along with any action taken or not taken by the controller in response to the appeal and the controller's written explanation of the reasons in support thereof, to the attorney general.

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

6.5 / MN / 1

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than sixty days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

CT

pg 12

6.5/CT/1

(3) (a) A CONTROLLER SHALL ESTABLISH AN INTERNAL PROCESS WHEREBY CONSUMERS MAY APPEAL A REFUSAL TO TAKE ACTION ON A REQUEST TO EXERCISE ANY OF THE RIGHTS UNDER SUBSECTION (1) OF THIS SECTION WITHIN A REASONABLE PERIOD AFTER THE CONSUMER'S RECEIPT OF THE NOTICE SENT BY THE CONTROLLER UNDER SUBSECTION (2)(b) OF THIS SECTION. THE APPEAL PROCESS MUST BE CONSPICUOUSLY AVAILABLE AND AS EASY TO USE AS THE PROCESS FOR SUBMITTING A REQUEST UNDER THIS SECTION.

CO
Pg 21

(b) WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF AN APPEAL, A CONTROLLER SHALL INFORM THE CONSUMER OF ANY ACTION TAKEN OR NOT TAKEN IN RESPONSE TO THE APPEAL, ALONG WITH A WRITTEN EXPLANATION OF THE REASONS IN SUPPORT OF THE RESPONSE. THE CONTROLLER MAY EXTEND THE FORTY-FIVE-DAY PERIOD BY SIXTY ADDITIONAL DAYS WHERE REASONABLY NECESSARY, TAKING INTO ACCOUNT THE COMPLEXITY AND NUMBER OF REQUESTS SERVING AS THE BASIS FOR THE APPEAL. THE CONTROLLER SHALL INFORM THE CONSUMER OF AN EXTENSION WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE APPEAL, TOGETHER WITH THE REASONS FOR THE DELAY.

CO
P 22

(c) THE CONTROLLER SHALL INFORM THE CONSUMER OF THE CONSUMER'S ABILITY TO CONTACT THE ATTORNEY GENERAL IF THE CONSUMER HAS CONCERNS ABOUT THE RESULT OF THE APPEAL.

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, 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 such information.

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

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

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

Sec. 9. (NEW) (*Effective July 1, 2023*) (a) Any controller in possession of de-identified data shall: (1) Take reasonable measures to ensure that the data cannot be associated with an individual; (2) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and (3) contractually obligate any recipients of the de-identified data to comply with all provisions of sections 1 to 11, inclusive, of this act.

(b) Nothing in sections 1 to 11, inclusive, of this act shall be construed to: (1) Require a controller or processor to re-identify de-identified data or pseudonymous data; or (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.

(c) Nothing in sections 1 to 11, inclusive, of this act shall be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller: (1) 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; (2) 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 (3) 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.

(d) The rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 4 of this act shall not apply to pseudonymous data in cases where the controller is able to demonstrate that 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 such information. 20

(e) A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments. 21

6-1-1307. Processing de-identified data. (1) THIS PART 13 DOES NOT REQUIRE A CONTROLLER OR PROCESSOR TO DO ANY OF THE FOLLOWING SOLELY FOR PURPOSES OF COMPLYING WITH THIS PART 13:

(a) REIDENTIFY DE-IDENTIFIED DATA;

(b) COMPLY WITH AN AUTHENTICATED CONSUMER REQUEST TO ACCESS, CORRECT, DELETE, OR PROVIDE PERSONAL DATA IN A PORTABLE FORMAT PURSUANT TO SECTION 6-1-1306 (1), IF ALL OF THE FOLLOWING ARE TRUE:

(I) (A) THE CONTROLLER IS NOT REASONABLY CAPABLE OF ASSOCIATING THE REQUEST WITH THE PERSONAL DATA; OR

(B) 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, EXCEPT AS OTHERWISE AUTHORIZED BY THE CONSUMER; OR

(c) MAINTAIN DATA IN IDENTIFIABLE FORM OR COLLECT, OBTAIN, RETAIN, OR ACCESS ANY DATA OR TECHNOLOGY IN ORDER TO ENABLE THE CONTROLLER TO ASSOCIATE AN AUTHENTICATED CONSUMER REQUEST WITH PERSONAL DATA. 22

(2) A CONTROLLER THAT USES DE-IDENTIFIED DATA SHALL EXERCISE REASONABLE OVERSIGHT TO MONITOR COMPLIANCE WITH ANY CONTRACTUAL COMMITMENTS TO WHICH THE DE-IDENTIFIED DATA ARE SUBJECT AND SHALL TAKE APPROPRIATE STEPS TO ADDRESS ANY BREACHES OF CONTRACTUAL COMMITMENTS.

(3) THE RIGHTS CONTAINED IN SECTION 6-1-1306 (1)(b) TO (1)(e) DO NOT APPLY TO PSEUDONYMOUS DATA IF THE CONTROLLER CAN DEMONSTRATE THAT THE 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. 23

Responsibilities of Controllers (Privacy Notice)

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

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

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

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

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

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

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

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

(7) the length of time the controller intends to retain each category of personal data or the criteria used to determine the length of time the controller intends to retain categories of personal data;

(8) if a controller engages in profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer:

(i) what decisions are subject to such profiling;

(ii) how profiling is used in the decision-making process, including the role of human involvement, if any; and

(iii) the benefits and potential consequences of the decision concerning the consumer; and

(9) the date the privacy notice was last updated.

(b) If a controller sells personal data to third parties, processes personal data for targeted advertising, or engages in profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer, it must disclose such processing in the privacy notice and provide access to a clear and conspicuous method outside the privacy notice for a consumer to opt out of the sale, processing, or profiling. This method may include but is not limited to an internet hyperlink clearly labeled

"Your Opt-Out Rights" or "Your Privacy Rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request.

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

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

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

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

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

(c) A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes: (1) The categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (4) the categories of personal data that the controller shares with third parties, if any; (5) the categories of third parties, if any, with which the controller shares personal data; and (6) an active electronic mail address or other online mechanism that the consumer may use to contact the controller.

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

CT

(e) (1) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to sections 1 to 11, inclusive, of this act. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to verify the identity of the consumer making the request.

pg 14

6-1-1308. Duties of controllers. (1) **Duty of transparency.** (a) A CONTROLLER SHALL PROVIDE CONSUMERS WITH A REASONABLY ACCESSIBLE, CLEAR, AND MEANINGFUL PRIVACY NOTICE THAT INCLUDES:

(I) THE CATEGORIES OF PERSONAL DATA COLLECTED OR PROCESSED BY THE CONTROLLER OR A PROCESSOR;

(II) THE PURPOSES FOR WHICH THE CATEGORIES OF PERSONAL DATA ARE PROCESSED;

(III) HOW AND WHERE CONSUMERS MAY EXERCISE THE RIGHTS PURSUANT TO SECTION 6-1-1306, INCLUDING THE CONTROLLER'S CONTACT INFORMATION AND HOW A CONSUMER MAY APPEAL A CONTROLLER'S ACTION WITH REGARD TO THE CONSUMER'S REQUEST;

(IV) THE CATEGORIES OF PERSONAL DATA THAT THE CONTROLLER SHARES WITH THIRD PARTIES, IF ANY; AND

CO
pg 23

(V) THE CATEGORIES OF THIRD PARTIES, IF ANY, WITH WHOM THE CONTROLLER SHARES PERSONAL DATA.

(b) IF A CONTROLLER SELLS PERSONAL DATA TO THIRD PARTIES OR PROCESSES PERSONAL DATA FOR TARGETED ADVERTISING, THE CONTROLLER SHALL CLEARLY AND CONSPICUOUSLY DISCLOSE THE SALE OR PROCESSING, AS WELL AS THE MANNER IN WHICH A CONSUMER MAY EXERCISE THE RIGHT TO OPT OUT OF THE SALE OR PROCESSING.

8.1 CO 11

(c) A CONTROLLER SHALL NOT:

(I) REQUIRE A CONSUMER TO CREATE A NEW ACCOUNT IN ORDER TO EXERCISE A RIGHT; OR

(II) BASED SOLELY ON THE EXERCISE OF A RIGHT AND UNRELATED TO FEASIBILITY OR THE VALUE OF A SERVICE, INCREASE THE COST OF, OR DECREASE THE AVAILABILITY OF, THE PRODUCT OR SERVICE.

CO

Pg 24

(d) NOTHING IN THIS PART 13 SHALL BE CONSTRUED TO REQUIRE A CONTROLLER TO PROVIDE A PRODUCT OR SERVICE THAT REQUIRES THE PERSONAL DATA OF A CONSUMER THAT THE CONTROLLER DOES NOT COLLECT OR MAINTAIN OR TO 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 OFFER IS RELATED TO A CONSUMER'S VOLUNTARY PARTICIPATION IN A BONA FIDE LOYALTY, REWARDS, PREMIUM FEATURES, DISCOUNT, OR CLUB CARD PROGRAM.

8.1 | CO | 2

USE OF DATA

Subd. 2. **Use of data.** (a) A controller's collection of personal data must be limited to what is reasonably necessary in relation to the purposes for which such data are processed.

(b) A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the purposes for which such data are processed, as disclosed to the consumer.

(c) Except as provided in this chapter, a controller may not process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which

8,2 | MN | |

such personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

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

(e) 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.

(f) 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 such request.

(g) 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 consumer is a known child between the ages of 13 and 16.

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 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 such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.

Sec. 6. (NEW) (*Effective July 1, 2023*) (a) A controller shall: (1) Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer; (2) except as otherwise provided in sections 1 to 11, inclusive, of this act, not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent; (3) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue; (4) not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA; (5) not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers; (6) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; and (7) 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 a controller has actual knowledge, and wilfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 1 to 11, inclusive, of this act, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods

8,2/CT/1

or services to the consumer.

(b) Nothing in subsection (a) of this section shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or 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.

14

8, 2 / CT / 2

(2) **Duty of purpose specification.** A CONTROLLER SHALL SPECIFY THE EXPRESS PURPOSES FOR WHICH PERSONAL DATA ARE COLLECTED AND PROCESSED.

(3) **Duty of data minimization.** A CONTROLLER'S COLLECTION OF PERSONAL DATA MUST BE ADEQUATE, RELEVANT, AND LIMITED TO WHAT IS REASONABLY NECESSARY IN RELATION TO THE SPECIFIED PURPOSES FOR WHICH THE DATA ARE PROCESSED.

CO
pg 24

(4) **Duty to avoid secondary use.** A CONTROLLER SHALL NOT PROCESS PERSONAL DATA FOR PURPOSES THAT ARE NOT REASONABLY NECESSARY TO OR COMPATIBLE WITH THE SPECIFIED PURPOSES FOR WHICH THE PERSONAL DATA ARE PROCESSED, UNLESS THE CONTROLLER FIRST OBTAINS THE CONSUMER'S CONSENT.

(5) **Duty of care.** A CONTROLLER SHALL TAKE REASONABLE MEASURES TO SECURE PERSONAL DATA DURING BOTH STORAGE AND USE FROM UNAUTHORIZED ACQUISITION. THE DATA SECURITY PRACTICES MUST BE APPROPRIATE TO THE VOLUME, SCOPE, AND NATURE OF THE PERSONAL DATA PROCESSED AND THE NATURE OF THE BUSINESS.

(6) **Duty to avoid unlawful discrimination.** A CONTROLLER SHALL NOT PROCESS PERSONAL DATA IN VIOLATION OF STATE OR FEDERAL LAWS THAT PROHIBIT UNLAWFUL DISCRIMINATION AGAINST CONSUMERS.

CO
pg 25

(7) **Duty regarding sensitive data.** A CONTROLLER SHALL NOT PROCESS A CONSUMER'S SENSITIVE DATA WITHOUT FIRST OBTAINING THE CONSUMER'S CONSENT OR, IN THE CASE OF THE PROCESSING OF PERSONAL DATA CONCERNING A KNOWN CHILD, WITHOUT FIRST OBTAINING CONSENT FROM THE CHILD'S PARENT OR LAWFUL GUARDIAN.

WAIVER OF RIGHTS UNENFORCEABL

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

MN

8.4 / MN / 1

DATA PRIVACY ASSESSMENTS

Sec. 9. **[325O.08] DATA PRIVACY AND PROTECTION ASSESSMENTS.**

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

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

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

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

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

(iii) maintain the accuracy and integrity of personal data subject to this act;

(iv) prevent the collection of personal data that is not necessary to provide services which have been requested by the consumer;

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

9/MN/1

(vi) identify and remediate violations of this act;

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

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

(ii) the sale of personal data;

(iii) the processing of sensitive data;

(iv) any processing activities involving personal data that present a heightened risk of harm to consumers; and

(v) the processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

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

(B) financial, physical, or reputational injury to consumers;

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or

(D) other substantial injury to consumers; and

(4) a description of the data dictionary, metadata catalog, or other means by which the controller maintains its inventory of data that must be managed to exercise its responsibilities under section 325O.05.

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

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

(d) The attorney general may request, in writing, that a controller disclose any data privacy and protection assessment that is relevant to an investigation conducted by the attorney general. The controller must make a data privacy and protection assessment available to the attorney general upon such a request. The attorney general may evaluate the data privacy and protection assessments for compliance with the responsibilities contained in section 325O.07 and with other laws. Data privacy and protection assessments are classified as nonpublic data, as defined by section 13.02, subdivision 9. The disclosure of a data privacy and protection assessment pursuant to a request from the attorney general under this paragraph does not constitute a waiver of the attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

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

Sec. 8. (NEW) (*Effective July 1, 2023*) (a) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes: (1) The processing of personal data for the purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (B) financial, physical or reputational injury to consumers, (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or (D) other substantial injury to consumers; and (4) the processing of sensitive data.

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the

9/CT/1

consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in sections 1 to 11, inclusive, of this act. Data protection assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200 of the general statutes. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(f) Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2023, and are not retroactive.

6-1-1309. Data protection assessments - attorney general access and evaluation - definition. (1) A CONTROLLER SHALL NOT CONDUCT PROCESSING THAT PRESENTS A HEIGHTENED RISK OF HARM TO A CONSUMER WITHOUT CONDUCTING AND DOCUMENTING A DATA PROTECTION ASSESSMENT OF EACH OF ITS PROCESSING ACTIVITIES THAT INVOLVE PERSONAL DATA ACQUIRED ON OR AFTER THE EFFECTIVE DATE OF THIS SECTION THAT PRESENT A HEIGHTENED RISK OF HARM TO A CONSUMER.

(2) FOR PURPOSES OF THIS SECTION, "PROCESSING THAT PRESENTS A HEIGHTENED RISK OF HARM TO A CONSUMER" INCLUDES THE FOLLOWING:

(a) PROCESSING PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR FOR PROFILING IF THE PROFILING PRESENTS A REASONABLY FORESEEABLE RISK OF:

(I) UNFAIR OR DECEPTIVE TREATMENT OF, OR UNLAWFUL DISPARATE IMPACT ON, CONSUMERS;

(II) FINANCIAL OR PHYSICAL INJURY TO CONSUMERS;

(III) A PHYSICAL OR OTHER INTRUSION UPON THE SOLITUDE OR SECLUSION, OR THE PRIVATE AFFAIRS OR CONCERNS, OF CONSUMERS IF THE INTRUSION WOULD BE OFFENSIVE TO A REASONABLE PERSON; OR

(IV) OTHER SUBSTANTIAL INJURY TO CONSUMERS;

(b) SELLING PERSONAL DATA; AND

(c) PROCESSING SENSITIVE DATA.

(3) DATA PROTECTION ASSESSMENTS MUST IDENTIFY AND WEIGH THE BENEFITS THAT MAY FLOW, DIRECTLY AND INDIRECTLY, FROM THE PROCESSING TO THE CONTROLLER, THE CONSUMER, OTHER STAKEHOLDERS, AND THE PUBLIC AGAINST THE POTENTIAL RISKS TO THE RIGHTS OF THE CONSUMER ASSOCIATED WITH THE PROCESSING, AS MITIGATED BY SAFEGUARDS THAT THE CONTROLLER CAN EMPLOY TO REDUCE THE RISKS. THE CONTROLLER SHALL FACTOR INTO THIS ASSESSMENT THE USE OF DE-IDENTIFIED DATA AND THE REASONABLE EXPECTATIONS OF CONSUMERS, AS WELL AS THE CONTEXT OF THE PROCESSING AND THE RELATIONSHIP BETWEEN THE CONTROLLER AND THE CONSUMER WHOSE PERSONAL DATA WILL BE PROCESSED.

(4) A CONTROLLER SHALL MAKE THE DATA PROTECTION ASSESSMENT AVAILABLE TO THE ATTORNEY GENERAL UPON REQUEST. THE ATTORNEY GENERAL MAY EVALUATE THE DATA PROTECTION ASSESSMENT FOR COMPLIANCE WITH THE DUTIES CONTAINED IN SECTION 6-1-1308 AND WITH OTHER LAWS, INCLUDING THIS ARTICLE 1. DATA PROTECTION ASSESSMENTS ARE CONFIDENTIAL AND EXEMPT FROM PUBLIC INSPECTION AND COPYING UNDER THE "COLORADO OPEN RECORDS ACT", PART 2 OF ARTICLE 72 OF TITLE 24. THE DISCLOSURE OF A DATA PROTECTION ASSESSMENT PURSUANT TO A REQUEST FROM THE ATTORNEY GENERAL UNDER THIS SUBSECTION (4) DOES NOT CONSTITUTE A WAIVER OF ANY ATTORNEY-CLIENT PRIVILEGE OR WORK-PRODUCT PROTECTION THAT MIGHT OTHERWISE EXIST WITH RESPECT TO THE ASSESSMENT AND ANY INFORMATION CONTAINED IN THE ASSESSMENT.

(5) A SINGLE DATA PROTECTION ASSESSMENT MAY ADDRESS A COMPARABLE SET OF PROCESSING OPERATIONS THAT INCLUDE SIMILAR ACTIVITIES.

26

(6) DATA PROTECTION ASSESSMENT REQUIREMENTS APPLY TO PROCESSING ACTIVITIES CREATED OR GENERATED AFTER JULY 1, 2023, AND ARE NOT RETROACTIVE.

LIMITATIONS AND APPLICABILITY

Sec. 10. **[325O.09] LIMITATIONS AND APPLICABILITY.**

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

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

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

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

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

(5) provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;

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

(7) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity

10/MN/1

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

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

(9) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity which has determined that:

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

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

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

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

(2) perform solely 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 when those internal operations are performed during, and not following, the consumer's relationship with the controller.

(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 such 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

10/MN/2

with the requirements of this chapter is likewise not in violation of this chapter for the obligations of the controller or processor from which it receives such personal data.

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

(1) adversely affect the rights or freedoms of any persons, such as 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 must not be processed for any purpose other than those expressly listed in this section. Personal data that are processed by a controller pursuant to this section may be processed solely to the extent that such 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 such 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 such processing.

Sec. 10. (NEW) (*Effective July 1, 2023*) (a) Nothing in sections 1 to 11, inclusive, of this act shall be construed to restrict a controller's or processor's ability to: (1) Comply with federal, state or municipal ordinances or regulations; (2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities; (3) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations; (4) investigate, establish, exercise, prepare for or defend legal claims; (5) provide a product or service specifically requested by a consumer; (6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty; (7) take steps at the request of a consumer prior to entering into a contract; (8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis; (9) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action; (10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar

independent oversight entities that determine, (A) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller, (B) the expected benefits of the research outweigh the privacy risks, and (C) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification; (11) assist another controller, processor or third party with any of the obligations under sections 1 to 11, inclusive, of this act; or (12) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is (A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(b) The obligations imposed on controllers or processors under sections 1 to 11, inclusive, of this act shall not restrict a controller's or processor's ability to collect, use or retain data for internal use to: (1) Conduct internal research to develop, improve or repair products, services or technology; (2) effectuate a product recall; (3) identify and repair technical errors that impair existing or intended functionality; or (4) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data 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.

(c) The obligations imposed on controllers or processors under sections 1 to 11, inclusive, of this act shall not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this state. Nothing in sections 1 to 11, inclusive, of this act shall be construed to prevent a controller or

10/CT/2

processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

(d) A controller or processor that discloses personal data to a processor or third-party controller in accordance with sections 1 to 11, inclusive, of this act shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes such personal data violates said sections, provided, at the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller would violate said sections. A third-party controller or processor receiving personal data from a controller or processor in compliance with sections 1 to 11, inclusive, of this act is likewise not in violation of said sections for the transgressions of the controller or processor from which such third-party controller or processor receives such personal data.

(e) Nothing in sections 1 to 11, inclusive, of this act shall be construed to: (1) Impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person (A) to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution, or (B) under section 52-146t of the general statutes; or (2) apply to any person's processing of personal data in the course of such person's purely personal or household activities.

(f) Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is: (1) Reasonably necessary and proportionate to the purposes listed in this section; and (2) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used or retained pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of such

10/CT/3

collection, use or retention. Such data shall be subject 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 relating to such collection, use or retention of personal data.

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

24

(h) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller with respect to such processing.

(3) THE OBLIGATIONS IMPOSED ON CONTROLLERS OR PROCESSORS UNDER THIS PART 13 DO NOT:

(a) RESTRICT A CONTROLLER'S OR PROCESSOR'S ABILITY TO:

P912

10/20/11

(I) COMPLY WITH FEDERAL, STATE, OR LOCAL LAWS, RULES, OR REGULATIONS;

(II) COMPLY WITH A CIVIL, CRIMINAL, OR REGULATORY INQUIRY, INVESTIGATION, SUBPOENA, OR SUMMONS BY FEDERAL, STATE, LOCAL, OR OTHER GOVERNMENTAL AUTHORITIES;

(III) COOPERATE WITH LAW ENFORCEMENT AGENCIES CONCERNING CONDUCT OR ACTIVITY THAT THE CONTROLLER OR PROCESSOR REASONABLY AND IN GOOD FAITH BELIEVES MAY VIOLATE FEDERAL, STATE, OR LOCAL LAW;

(IV) INVESTIGATE, EXERCISE, PREPARE FOR, OR DEFEND ACTUAL OR ANTICIPATED LEGAL CLAIMS;

(V) CONDUCT INTERNAL RESEARCH TO IMPROVE, REPAIR, OR DEVELOP PRODUCTS, SERVICES, OR TECHNOLOGY;

(VI) IDENTIFY AND REPAIR TECHNICAL ERRORS THAT IMPAIR EXISTING OR INTENDED FUNCTIONALITY;

(VII) PERFORM INTERNAL OPERATIONS THAT ARE REASONABLY ALIGNED WITH THE EXPECTATIONS OF THE CONSUMER BASED ON THE CONSUMER'S EXISTING RELATIONSHIP WITH THE CONTROLLER;

(VIII) PROVIDE A PRODUCT OR SERVICE SPECIFICALLY REQUESTED BY A CONSUMER OR THE PARENT OR GUARDIAN OF A CHILD, PERFORM A CONTRACT TO WHICH THE CONSUMER IS A PARTY, OR TAKE STEPS AT THE REQUEST OF THE CONSUMER PRIOR TO ENTERING INTO A CONTRACT;

(IX) PROTECT THE VITAL INTERESTS OF THE CONSUMER OR OF ANOTHER INDIVIDUAL;

(X) PREVENT, DETECT, PROTECT AGAINST, OR RESPOND TO SECURITY INCIDENTS, IDENTITY THEFT, FRAUD, HARASSMENT, OR MALICIOUS, DECEPTIVE, OR ILLEGAL ACTIVITY; PRESERVE THE INTEGRITY OR SECURITY OF SYSTEMS; OR INVESTIGATE, REPORT, OR PROSECUTE THOSE RESPONSIBLE FOR ANY SUCH ACTION;

(XI) PROCESS PERSONAL DATA FOR REASONS OF PUBLIC INTEREST IN

THE AREA OF PUBLIC HEALTH, BUT SOLELY TO THE EXTENT THAT THE PROCESSING:

(A) IS SUBJECT TO SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS OF THE CONSUMER WHOSE PERSONAL DATA ARE PROCESSED; AND

(B) IS UNDER THE RESPONSIBILITY OF A PROFESSIONAL SUBJECT TO CONFIDENTIALITY OBLIGATIONS UNDER FEDERAL, STATE, OR LOCAL LAW; OR

(XII) ASSIST ANOTHER PERSON WITH ANY OF THE ACTIVITIES SET FORTH IN THIS SUBSECTION (3);

(b) APPLY WHERE COMPLIANCE BY THE CONTROLLER OR PROCESSOR WITH THIS PART 13 WOULD VIOLATE AN EVIDENTIARY PRIVILEGE UNDER COLORADO LAW;

(c) PREVENT A CONTROLLER OR PROCESSOR FROM PROVIDING PERSONAL DATA CONCERNING A CONSUMER TO A PERSON COVERED BY AN EVIDENTIARY PRIVILEGE UNDER COLORADO LAW AS PART OF A PRIVILEGED COMMUNICATION;

(d) APPLY TO INFORMATION MADE AVAILABLE BY A THIRD PARTY THAT THE CONTROLLER HAS A REASONABLE BASIS TO BELIEVE IS PROTECTED SPEECH PURSUANT TO APPLICABLE LAW; AND

(e) APPLY TO THE PROCESSING OF PERSONAL DATA BY AN INDIVIDUAL IN THE COURSE OF A PURELY PERSONAL OR HOUSEHOLD ACTIVITY.

(4) PERSONAL DATA THAT ARE PROCESSED BY A CONTROLLER PURSUANT TO AN EXCEPTION PROVIDED BY THIS SECTION:

(a) SHALL NOT BE PROCESSED FOR ANY PURPOSE OTHER THAN A PURPOSE EXPRESSLY LISTED IN THIS SECTION OR AS OTHERWISE AUTHORIZED BY THIS PART 13; AND

(b) SHALL BE PROCESSED SOLELY TO THE EXTENT THAT THE PROCESSING IS NECESSARY, REASONABLE, AND PROPORTIONATE TO THE SPECIFIC PURPOSE OR PURPOSES LISTED IN THIS SECTION OR AS OTHERWISE

10/CO/3

AUTHORIZED BY THIS PART 13.

(5) 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 SUBSECTION (4) OF THIS SECTION.

(D pg 15

10/co/4

AG Enforcement

Sec. 11. **[325O.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.

11/MN/1

Sec. 11. (NEW) (*Effective July 1, 2023*) (a) The Attorney General shall have exclusive authority to enforce violations of sections 1 to 10, inclusive, of this act.

(b) During the period beginning on July 1, 2023, and ending on December 31, 2024, the Attorney General shall, prior to initiating any action for a violation of any provision of sections 1 to 10, inclusive, of this act, issue a notice of violation to the controller if the Attorney General determines that a cure is possible. If the controller fails to cure such violation within sixty days of receipt of the notice of violation, the Attorney General may bring an action pursuant to this section. Not later than February 1, 2024, the Attorney General shall submit a report, in accordance with section 11-4a of the general statutes, to the joint standing committee of the General Assembly having cognizance of matters relating to general law disclosing: (1) The number of notices of violation the Attorney General has issued; (2) the nature of each violation; (3) the number of violations that were cured during the sixty-day cure period; and (4) any other matter the Attorney General deems relevant for the purposes of such report. CO 24

(c) Beginning on January 1, 2025, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation described in subsection (b) of this section, consider: (1) The number of violations; (2) the size and complexity of the controller or processor; (3) the nature and extent of the controller's or processor's processing activities; (4) the substantial likelihood of injury to the public; (5) the safety of persons or property; and (6) whether such alleged violation was likely caused by human or technical error.

(d) Nothing in sections 1 to 10, inclusive, of this act shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or any other law.

(e) A violation of the requirements of sections 1 to 10, inclusive, of this act shall constitute an unfair trade practice for purposes of section 42-110b of the general statutes and shall be enforced solely by the Attorney General, provided the provisions of section 42-110g of the general statutes shall not apply to such violation. CO 25

6-1-1310. Liability. (1) NOTWITHSTANDING ANY PROVISION IN PART 1 OF THIS ARTICLE 1, THIS PART 13 DOES NOT AUTHORIZE A PRIVATE RIGHT OF ACTION FOR A VIOLATION OF THIS PART 13 OR ANY OTHER PROVISION OF LAW. THIS SUBSECTION (1) NEITHER RELIEVES ANY PARTY FROM ANY DUTIES OR OBLIGATIONS IMPOSED, NOR ALTERS ANY INDEPENDENT RIGHTS THAT CONSUMERS HAVE, UNDER OTHER LAWS, INCLUDING THIS ARTICLE 1, THE STATE CONSTITUTION, OR THE UNITED STATES CONSTITUTION.

CO 26

(2) WHERE MORE THAN ONE CONTROLLER OR PROCESSOR, OR BOTH A CONTROLLER AND A PROCESSOR, INVOLVED IN THE SAME PROCESSING VIOLATES THIS PART 13, THE LIABILITY SHALL BE ALLOCATED AMONG THE PARTIES ACCORDING TO PRINCIPLES OF COMPARATIVE FAULT.

6-1-1311. Enforcement - penalties - repeal. (1) (a) NOTWITHSTANDING ANY OTHER PROVISION OF THIS ARTICLE 1, THE ATTORNEY GENERAL AND DISTRICT ATTORNEYS HAVE EXCLUSIVE AUTHORITY TO ENFORCE THIS PART 13 BY BRINGING AN ACTION IN THE NAME OF THE STATE OR AS PARENS PATRIAE ON BEHALF OF PERSONS RESIDING IN THE STATE TO ENFORCE THIS PART 13 AS PROVIDED IN THIS ARTICLE 1, INCLUDING SEEKING AN INJUNCTION TO ENJOIN A VIOLATION OF THIS PART 13.

CO 27

(b) NOTWITHSTANDING ANY OTHER PROVISION OF THIS ARTICLE 1, NOTHING IN THIS PART 13 SHALL BE CONSTRUED AS PROVIDING THE BASIS FOR, OR BEING SUBJECT TO, A PRIVATE RIGHT OF ACTION FOR VIOLATIONS OF THIS PART 13 OR ANY OTHER LAW.

(c) FOR PURPOSES ONLY OF ENFORCEMENT OF THIS PART 13 BY THE ATTORNEY GENERAL OR A DISTRICT ATTORNEY, A VIOLATION OF THIS PART 13 IS A DECEPTIVE TRADE PRACTICE.

(d) PRIOR TO ANY ENFORCEMENT ACTION PURSUANT TO SUBSECTION (1)(a) OF THIS SECTION, THE ATTORNEY GENERAL OR DISTRICT ATTORNEY MUST ISSUE A NOTICE OF VIOLATION TO THE CONTROLLER IF A CURE IS DEEMED POSSIBLE. IF THE CONTROLLER FAILS TO CURE THE VIOLATION WITHIN SIXTY DAYS AFTER RECEIPT OF THE NOTICE OF VIOLATION, AN ACTION MAY BE BROUGHT PURSUANT TO THIS SECTION. THIS SUBSECTION (1)(d) IS REPEALED, EFFECTIVE JANUARY 1, 2025.

(2) THE STATE TREASURER SHALL CREDIT ALL RECEIPTS FROM THE IMPOSITION OF CIVIL PENALTIES UNDER THIS PART 13 PURSUANT TO SECTION 24-31-108.

SECTION 2. In Colorado Revised Statutes, **amend** 6-1-104 as follows:

6-1-104. Cooperative reporting. The district attorneys may cooperate in a statewide reporting system by receiving, on forms provided by the attorney general, complaints from persons concerning deceptive trade practices listed in section 6-1-105 ~~and~~ OR part 7 OR 13 of this ~~article~~ ARTICLE 1 and transmitting ~~such~~ THE complaints to the attorney general.

SECTION 3. In Colorado Revised Statutes, 6-1-105, **add** (1)(nnn) as follows:

6-1-105. Unfair or deceptive trade practices. (1) A person engages in a deceptive trade practice when, in the course of the person's business, vocation, or occupation, the person:

C029

(nnn) VIOLATES ANY PROVISION OF PART 13 OF THIS ARTICLE 1 AS SPECIFIED IN SECTION 6-1-1311 (1)(c).

SECTION 4. In Colorado Revised Statutes, 6-1-107, **amend** (1) introductory portion as follows:

6-1-107. Powers of attorney general and district attorneys. (1) When the attorney general or a district attorney has reasonable cause to believe that any person, whether in this state or elsewhere, has engaged in or is engaging in any deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this ~~article~~ ARTICLE 1, the attorney general or district attorney may:

11/10/2

SECTION 5. In Colorado Revised Statutes, 6-1-108, **amend** (1) as follows:

6-1-108. Subpoenas - hearings - rules. (1) When the attorney general or a district attorney has reasonable cause to believe that a person, whether in this state or elsewhere, has engaged in or is engaging in a deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this article 1, the attorney general or a district attorney, in addition to other powers conferred upon ~~him or her~~ THE ATTORNEY GENERAL OR A DISTRICT ATTORNEY by this article 1, may issue subpoenas to require the attendance of witnesses or the production of documents, administer oaths, conduct hearings in aid of any investigation or inquiry, and prescribe such forms and promulgate such rules as may be necessary to administer the provisions of this article 1.

SECTION 6. In Colorado Revised Statutes, 6-1-110, **amend** (1) and (2) as follows:

6-1-110. Restraining orders - injunctions - assurances of discontinuance. (1) Whenever the attorney general or a district attorney has cause to believe that a person has engaged in or is engaging in any deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this ~~article~~ ARTICLE 1, the attorney general or district attorney may apply for and obtain, in an action in the appropriate district court of this state, a temporary restraining order or injunction, or both, pursuant to the Colorado rules of civil procedure, prohibiting ~~such~~ THE person from continuing ~~such~~ THE practices, or engaging therein, or doing any act in furtherance thereof. The court may make such orders or judgments as may be necessary to prevent the use or employment by ~~such~~ THE person of any such deceptive trade practice or ~~which~~ THAT may be necessary to completely compensate or restore to the original position of any person injured by means of any such practice or to prevent any unjust enrichment by any person through the use or employment of any deceptive trade practice.

CO 30

(2) Where the attorney general or a district attorney has authority to institute a civil action or other proceeding pursuant to the provisions of this ~~article~~ ARTICLE 1, the attorney general or district attorney may accept, in lieu thereof or as a part thereof, an assurance of discontinuance of any deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this ~~article. Such~~ ARTICLE 1. THE assurance may include a stipulation for the voluntary

11/20/13

payment by the alleged violator of the costs of investigation and any action or proceeding by the attorney general or a district attorney and any amount necessary to restore to any person any money or property that may have been acquired by ~~such~~ THE alleged violator by means of any such deceptive trade practice. Any such assurance of discontinuance accepted by the attorney general or a district attorney and any such stipulation filed with the court as a part of any such action or proceeding ~~shall be~~ IS a matter of public record unless the attorney general or the district attorney determines, at ~~his or her~~ THE discretion OF THE ATTORNEY GENERAL OR DISTRICT ATTORNEY, that it will be confidential to the parties to the action or proceeding and to the court and its employees. Upon the filing of a civil action by the attorney general or a district attorney alleging that a confidential assurance of discontinuance or stipulation accepted pursuant to this subsection (2) has been violated, ~~said~~ THE assurance of discontinuance or stipulation ~~shall thereupon be deemed~~ BECOMES a public record and open to inspection by any person. Proof by a preponderance of the evidence of a violation of any such assurance or stipulation ~~shall constitute~~ CONSTITUTES prima facie evidence of a deceptive trade practice for the purposes of any civil action or proceeding brought thereafter by the attorney general or a district attorney, whether a new action or a subsequent motion or petition in any pending action or proceeding.

CO
31

SECTION 7. Act subject to petition - effective date - applicability. (1) This act takes effect July 1, 2023; except that, if a referendum petition is filed pursuant to section 1 (3) of article V of the state constitution against this act or an item, section, or part of this act within the ninety-day period after final adjournment of the general assembly, then the act, item, section, or part will not take effect unless approved by the people at the general election to be held in November 2022 and, in such case, will take effect July 1, 2023, or on the date of the official declaration of the vote thereon by the governor, whichever is later.

PREEMPTION OF LOCAL LAW

Sec. 12. **[325O.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 act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

6-1-1312. Preemption - local governments. THIS PART 13 SUPERSEDES AND PREEMPTS LAWS, ORDINANCES, RESOLUTIONS, REGULATIONS, OR THE EQUIVALENT ADOPTED BY ANY STATUTORY OR HOME RULE MUNICIPALITY, COUNTY, OR CITY AND COUNTY REGARDING THE PROCESSING OF PERSONAL DATA BY CONTROLLERS OR PROCESSORS.

27

12/MN CO/1

EFFECTIVE DATE

Sec. 13. **EFFECTIVE DATE.**

This act ~~is effective July 31, 2024, except that postsecondary institutions regulated by~~ the Office of Higher Education and nonprofit corporations governed by Minnesota Statutes, chapter 317A, are not required to comply with this act until July 31, 2028.

13/MN/1

Task Forces

Sec. 12. (*Effective from passage*) (a) Not later than September 1, 2022, the chairpersons of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall convene a task force to study:

(1) Information sharing among health care providers and social care providers and make recommendations to eliminate health disparities and inequities across sectors, as described in subsection (a) of section 19a-133b of the general statutes;

(2) Algorithmic decision-making and make recommendations concerning the proper use of data to reduce bias in such decision-making;

(3) Possible legislation that would require an operator, as defined in the Children's Online Privacy Protection Act, 15 USC 6501 et seq., as

25

99/CT/11

amended from time to time, to, upon a parent's request, delete the account of a child and cease to collect, use or maintain, in retrievable form, the child's personal data on the operator's Internet web site or online service directed to children, and provide parents with an accessible, reasonable and verifiable means to make such a request;

(4) Any means available to verify the age of a child who creates a social media account;

(5) Issues concerning data colocation, including, but not limited to, the impact that the provisions of sections 1 to 11, inclusive, of this act have on third parties that provide data storage and colocation services;

(6) Possible legislation that would expand the provisions of sections 1 to 11, inclusive, of this act to include additional persons or groups; and

(7) Other topics concerning data privacy.

(b) The chairpersons of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall serve as the chairpersons of the task force, and shall jointly appoint the members of the task force. Such members shall include, but need not be limited to:

(1) Representatives from business, academia, consumer advocacy groups, small and large companies and the office of the Attorney General; and

(2) Attorneys with experience in privacy law.

(c) The administrative staff of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall serve as administrative staff of the task force.

(d) Not later than January 1, 2023, the task force shall submit a report on its findings and recommendations to the joint standing committee of

the General Assembly having cognizance of matters relating to general law, in accordance with the provisions of section 11-4a of the general statutes. The task force shall terminate on the date that it submits such report or January 1, 2023, whichever is later.

Approved May 10, 2022