1   TO THE HONORABLE SENATE:

2   The Committee on Economic Development, Housing and General Affairs to

3   which was referred House Bill No. 121 entitled "An act relating to enhancing

4   consumer privacy" respectfully reports that it has considered the same and

5   recommends that the Senate propose to the House that the bill be amended by

6   striking out all after the enacting clause and inserting in lieu thereof the

7   following:

8   Sec. 1. 9 V.S.A. chapter 61A is added to read:

9   CHAPTER 61A. VERMONT DATA PRIVACY ACT

10   § 2415. DEFINITIONS

11   As used in this chapter:

12   (1) "Abortion" has the same meaning as in section 2492 of this title.

13   (2)(A) "Affiliate" means a legal entity that shares common branding

14   with another legal entity or controls, is controlled by, or is under common

15   control with another legal entity.

16   (B) As used in subdivision (A) of this subdivision (2), "control" or

17   "controlled" means:

18   (i) ownership of, or the power to vote, more than 50 percent of the

19   outstanding shares of any class of voting security of a company;

20   (ii) control in any manner over the election of a majority of the

21   directors or of individuals exercising similar functions; or

1   (iii) the power to exercise controlling influence over the

2   management of a company.

3   (3) "Authenticate" means to use reasonable means to determine that a

4   request to exercise any of the rights afforded under subdivisions 2418(a)(1)–

5   (5) of this title is being made by, or on behalf of, the consumer who is entitled

6   to exercise the consumer rights with respect to the personal data at issue.

7   (4)(A) "Biometric data" means personal data generated from the

8   technological processing of an individual's unique biological, physical, or

9   physiological characteristics that is linked or reasonably linkable to an

10   individual, including:

11   (i) iris or retina scans;

12   (ii) fingerprints;

13   (iii) facial or hand mapping, geometry, or templates;

14   (iv) vein patterns;

15   (v) voice prints; and

16   (vi) gait or personally identifying physical movement or patterns.

17   (B) "Biometric data" does not include:

18   (i) a digital or physical photograph;

19   (ii) an audio or video recording; or

1　　　　　　　　(iii) any data generated from a digital or physical photograph, or

2　an audio or video recording, unless such data is generated to identify a specific

3　individual.

4　　　　　　(5) "Broker-dealer" has the same meaning as in 9 V.S.A. § 5102.

5　　　　　　(6) "Business associate" has the same meaning as in HIPAA.

6　　　　　　(7) "Child" has the same meaning as in COPPA.

7　　　　　　(8)(A) "Consent" means a clear affirmative act signifying a consumer's

8　freely given, specific, informed, and unambiguous agreement to allow the

9　processing of personal data relating to the consumer.

10　　　　　　(B) "Consent" may include a written statement, including by

11　electronic means, or any other unambiguous affirmative action.

12　　　　　　(C) "Consent" does not include:

13　　　　　　　(i) acceptance of a general or broad terms of use or similar

14　document that contains descriptions of personal data processing along with

15　other, unrelated information;

16　　　　　　　(ii) hovering over, muting, pausing, or closing a given piece of

17　content; or

18　　　　　　　(iii) agreement obtained through the use of dark patterns.

19　　　　　　(9)(A) "Consumer" means an individual who is a resident of the State.

20　　　　　　(B) "Consumer" does not include an individual acting in a

21　commercial or employment context or as an employee, owner, director, officer,

1   or contractor of a company, partnership, sole proprietorship, nonprofit, or

2   government agency whose communications or transactions with the controller

3   occur solely within the context of that individual's role with the company,

4   partnership, sole proprietorship, nonprofit, or government agency.

5   (10) "Consumer health data" means any personal data that a controller

6   uses to identify a consumer's physical or mental health condition or diagnosis,

7   including gender-affirming health data and reproductive or sexual health data.

8   (11) "Consumer health data controller" means any controller that, alone

9   or jointly with others, determines the purpose and means of processing

10   consumer health data.

11   (12) "Consumer reporting agency" has the same meaning as in the Fair

12   Credit Reporting Act, 15 U.S.C. § 1681a(f);

13   (13) "Controller" means a person who, alone or jointly with others,

14   determines the purpose and means of processing personal data.

15   (14) "COPPA" means the Children's Online Privacy Protection Act of

16   1998, 15 U.S.C. § 6501–6506, and any regulations, rules, guidance, and

17   exemptions promulgated pursuant to the act, as the act and regulations, rules,

18   guidance, and exemptions may be amended.

19   (15) "Covered entity" has the same meaning as in HIPAA.

20   (16) "Credit union" has the same meaning as in 8 V.S.A. § 30101.

1	(17) "Dark pattern" means a user interface designed or manipulated with

2	the substantial effect of subverting or impairing user autonomy, decision-

3	making, or choice and includes any practice the Federal Trade Commission

4	refers to as a "dark pattern."

5	(18) "Decisions that produce legal or similarly significant effects

6	concerning the consumer" means decisions made by the controller that result in

7	the provision or denial by the controller of financial or lending services,

8	housing, insurance, education enrollment or opportunity, criminal justice,

9	employment opportunities, health care services, or access to essential goods or

10	services.

11	(19) "De-identified data" means data that does not identify and cannot

12	reasonably be used to infer information about, or otherwise be linked to, an

13	identified or identifiable individual, or a device linked to the individual, if the

14	controller that possesses the data:

15	(A)(i) takes reasonable measures to ensure that the data cannot be

16	used to re-identify an identified or identifiable individual or be associated with

17	an individual or device that identifies or is linked or reasonably linkable to an

18	individual or household;

19	(ii) for purposes of this subdivision (A), "reasonable measures"

20	shall include the de-identification requirements set forth under 45 C.F.R.

1   § 164.514 (other requirements relating to uses and disclosures of protected

2   health information);

3   (B) publicly commits to process the data only in a de-identified

4   fashion and not attempt to re-identify the data; and

5   (C) contractually obligates any recipients of the data to satisfy the

6   criteria set forth in subdivisions (A) and (B) of this subdivision (19).

7   (20) "Educational institution" has the same meaning as "educational

8   agency or institution" in 20 U.S.C. § 1232g (family educational and privacy

9   rights);

10   (21) "Financial institution":

11   (A) as used in subdivision 2417(a)(12) of this title, has the same

12   meaning as in 15 U.S.C. § 6809; and

13   (B) as used in subdivision 2417(a)(14) of this title, has the same

14   meaning as in 8 V.S.A. § 11101.

15   (22) "Gender-affirming health care services" has the same meaning as in

16   1 V.S.A. § 150.

17   (23) "Gender-affirming health data" means any personal data

18   concerning a past, present, or future effort made by a consumer to seek, or a

19   consumer's receipt of, gender-affirming health care services, including:

20   (A) precise geolocation data that is used for determining a

21   consumer's attempt to acquire or receive gender-affirming health care services;

1   (B) efforts to research or obtain gender-affirming health care

2   services; and

3   (C) any gender-affirming health data that is derived from nonhealth

4   information.

5   (24) "Genetic data" means any data, regardless of its format, that results

6   from the analysis of a biological sample of an individual, or from another

7   source enabling equivalent information to be obtained, and concerns genetic

8   material, including deoxyribonucleic acids (DNA), ribonucleic acids (RNA),

9   genes, chromosomes, alleles, genomes, alterations or modifications to DNA or

10   RNA, single nucleotide polymorphisms (SNPs), epigenetic markers,

11   uninterpreted data that results from analysis of the biological sample or other

12   source, and any information extrapolated, derived, or inferred therefrom.

13   (25) "Geofence" means any technology that uses global positioning

14   coordinates, cell tower connectivity, cellular data, radio frequency

15   identification, wireless fidelity technology data, or any other form of location

16   detection, or any combination of such coordinates, connectivity, data,

17   identification, or other form of location detection, to establish a virtual

18   boundary.

19   (26) "Health care facility" has the same meaning as in 18 V.S.A. § 9432.

1   (27) "Heightened risk of harm to a minor" means processing the

2   personal data of a minor in a manner that presents a reasonably foreseeable risk

3   of:

4   (A) material physical or financial injury to a minor;

5   (B) emotional distress, as that term is defined in 13 V.S.A. § 1061(2),

6   to a minor;

7   (C) a highly offensive intrusion on the reasonable privacy

8   expectations of a minor;

9   (D) the encouragement of excessive or compulsive use of an online

10 service, product, or feature by a minor; or

11   (E) discrimination against the minor based upon the minor's race,

12 ethnicity, sex, disability, sexual orientation, gender identity, gender expression,

13 or national origin.

14   (28) "HIPAA" means the Health Insurance Portability and

15 Accountability Act of 1996, Pub. L. No. 104-191, and any regulations

16 promulgated pursuant to the act, as may be amended.

17   (29) "Identified or identifiable individual" means an individual who can

18 be readily identified, directly or indirectly, including by reference to an

19 identifier such as a name, an identification number, specific geolocation data,

20 or an online identifier.

1   (30) "Independent trust company" has the same meaning as in 8 V.S.A.

2   § 2401.

3   (31) "Investment adviser" has the same meaning as in 9 V.S.A. § 5102.

4   (32) "Mental health facility" means any health care facility in which at

5   least 70 percent of the health care services provided in the facility are mental

6   health services.

7   (33) "Nonpublic personal information" has the same meaning as in 15

8   U.S.C. § 6809.

9   (34)(A) "Online service, product, or feature" means any service,

10 product, or feature that is provided online, except as provided in subdivision

11 (B) of this subdivision (33).

12   (B) "Online service, product, or feature" does not include:

13   (i) telecommunications service, as that term is defined in the

14 Communications Act of 1934, 47 U.S.C. § 153;

15   (ii) broadband internet access service, as that term is defined in

16 47 C.F.R. § 54.400 (universal service support); or

17   (iii) the delivery or use of a physical product.

18   (35) "Patient identifying information" has the same meaning as in

19 42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

20   (36) "Patient safety work product" has the same meaning as in 42 C.F.R.

21 § 3.20 (patient safety organizations and patient safety work product).

1   (37)(A) "Personal data" means any information, including derived data

2   and unique identifiers, that is linked or reasonably linkable to an identified or

3   identifiable individual or to a device that identifies, is linked to, or is

4   reasonably linkable to one or more identified or identifiable individuals in a

5   household.

6   (B) "Personal data" does not include de-identified data or publicly

7   available information.

8   (38)(A) "Precise geolocation data" means personal data derived from

9   technology that accurately identifies within a radius of 1,850 feet a consumer's

10   present or past location or the present or past location of a device that links or

11   is linkable to a consumer or any data that is derived from a device that is used

12   or intended to be used to locate a consumer within a radius of 1,850 feet by

13   means of technology that includes a global positioning system that provides

14   latitude and longitude coordinates.

15   (B) "Precise geolocation data" does not include the content of

16   communications or any data generated by or connected to advanced utility

17   metering infrastructure systems or equipment for use by a utility.

18   (39) "Process" or "processing" means any operation or set of operations

19   performed, whether by manual or automated means, on personal data or on sets

20   of personal data, such as the collection, use, storage, disclosure, analysis,

21   deletion, or modification of personal data.

1   (40) "Processor" means a person who processes personal data on behalf

2   of a controller.

3   (41) "Profiling" means any form of automated processing performed on

4   personal data to evaluate, analyze, or predict personal aspects related to an

5   identified or identifiable individual's economic situation, health, personal

6   preferences, interests, reliability, behavior, location, or movements.

7   (42) "Protected health information" has the same meaning as in HIPAA.

8   (43) "Pseudonymous data" means personal data that cannot be attributed

9   to a specific individual without the use of additional information, provided the

10   additional information is kept separately and is subject to appropriate technical

11   and organizational measures to ensure that the personal data is not attributed to

12   an identified or identifiable individual.

13   (44) "Publicly available information" means information that:

14   (A) is lawfully made available through federal, state, or local

15   government records or widely distributed media; or

16   (B) a controller has a reasonable basis to believe a consumer has

17   lawfully made available to the general public.

18   (45) "Qualified service organization" has the same meaning as in 42

19   C.F.R. § 2.11 (confidentiality of substance use disorder patient records);

20   (46) "Reproductive or sexual health care" has the same meaning as

21   "reproductive health care services" in 1 V.S.A. § 150(c)(1).

1   (47) "Reproductive or sexual health data" means any personal data

2   concerning a past, present, or future effort made by a consumer to seek, or a

3   consumer's receipt of, reproductive or sexual health care.

4   (48) "Reproductive or sexual health facility" means any health care

5   facility in which at least 70 percent of the health care-related services or

6   products rendered or provided in the facility are reproductive or sexual health

7   care.

8   (49)(A) "Sale of personal data" means the exchange of a consumer's

9   personal data by the controller to a third party for monetary or other valuable

10   consideration.

11   (B) "Sale of personal data" does not include:

12   (i) the disclosure of personal data to a processor that processes the

13   personal data on behalf of the controller;

14   (ii) the disclosure of personal data to a third party for purposes of

15   providing a product or service requested by the consumer;

16   (iii) the disclosure or transfer of personal data to an affiliate of the

17   controller;

18   (iv) the disclosure of personal data where the consumer directs the

19   controller to disclose the personal data or intentionally uses the controller to

20   interact with a third party;

21   (v) the disclosure of personal data that the consumer:

1   (I) intentionally made available to the general public via a

2   channel of mass media; and

3   (II) did not restrict to a specific audience; or

4   (vi) the disclosure or transfer of personal data to a third party as an

5   asset that is part of a merger, acquisition, bankruptcy or other transaction, or a

6   proposed merger, acquisition, bankruptcy, or other transaction, in which the

7   third party assumes control of all or part of the controller's assets.

8   (50) "Sensitive data" means personal data that:

9   (A) reveals a consumer's government-issued identifier, such as a

10   Social Security number, passport number, state identification card, or driver's

11   license number, that is not required by law to be publicly displayed;

12   (B) reveals a consumer's racial or ethnic origin, national origin,

13   citizenship or immigration status, religious or philosophical beliefs, or union

14   membership;

15   (C) reveals a consumer's sexual orientation, sex life, sexuality, or

16   status as transgender or nonbinary;

17   (D) reveals a consumer's status as a victim of a crime;

18   (E) is financial information, including a consumer's tax return and

19   account number, financial account log-in, financial account, debit card number,

20   or credit card number in combination with any required security or access

21   code, password, or credentials allowing access to an account;

1   (F) is consumer health data;

2   (G) is personal data collected and analyzed concerning consumer

3   health data or personal data that describes or reveals a past, present, or future

4   mental or physical health condition, treatment, disability, or diagnosis,

5   including pregnancy, to the extent the personal data is not used by the

6   controller to identify a specific consumer's physical or mental health condition

7   or diagnosis;

8   (H) is biometric or genetic data;

9   (I) is personal data collected from a known child;

10   (J) is a photograph, film, video recording, or other similar medium

11 that shows the naked or undergarment-clad private area of a consumer; or

12   (K) is precise geolocation data.

13   (51)(A) "Targeted advertising" means displaying an advertisement to a

14 consumer where the advertisement is selected based on personal data obtained

15 or inferred from that consumer's activities over time and across nonaffiliated

16 internet websites or online applications to predict the consumer's preferences

17 or interests.

18   (B) "Targeted advertising" does not include:

19   (i) an advertisement based on activities within a controller's own

20 websites or online applications;

1   (ii) an advertisement based on the context of a consumer's current

2   search query, visit to a website, or use of an online application;

3   (iii) an advertisement directed to a consumer in response to the

4   consumer's request for information or feedback; or

5   (iv) processing personal data solely to measure or report

6   advertising frequency, performance, or reach.

7   (52) "Third party" means a person, such as a public authority, agency, or

8   body, other than the consumer, controller, or processor or an affiliate of the

9   processor or the controller.

10   (53) "Trade secret" has the same meaning as in section 4601 of this title.

11   (54) "Victim services organization" means a nonprofit organization that

12   is established to provide services to victims or witnesses of child abuse,

13   domestic violence, human trafficking, sexual assault, violent felony, or

14   stalking.

15   § 2416. APPLICABILITY

16   (a) Except as provided in subsection (b) of this section, this chapter applies

17   to a person that conducts business in this State or a person that produces

18   products or services that are targeted to residents of this State and that during

19   the preceding calendar year:

1   (1) controlled or processed the personal data of not fewer than 25,000

2   consumers, excluding personal data controlled or processed solely for the

3   purpose of completing a payment transaction; or

4   (2) derived more than 50 percent of the person's gross revenue from the

5   sale of personal data.

6   (b) Sections 2420 and 2426 of this title, and the provisions of this chapter

7   concerning consumer health data and consumer health data controllers apply to

8   a person that conducts business in this State or a person that produces products

9   or services that are targeted to residents of this State.

10   § 2417. EXEMPTIONS

11   (a) This chapter does not apply to:

12   (1) a federal, State, tribal, or local government entity in the ordinary

13   course of its operation;

14   (2) protected health information that a covered entity or business

15   associate processes in accordance with, or documents that a covered entity or

16   business associate creates for the purpose of complying with HIPAA;

17   (3) information used only for public health activities and purposes

18   described in 45 C.F.R. § 164.512 (disclosure of protected health information

19   without authorization);

20   (4) information that identifies a consumer in connection with:

1   (A) activities that are subject to the Federal Policy for the Protection

2   of Human Subjects, codified as 45 C.F.R. part 46 (HHS protection of human

3   subjects) and in various other federal regulations;

4   (B) research on human subjects undertaken in accordance with good

5   clinical practice guidelines issued by the International Council for

6   Harmonisation of Technical Requirements for Pharmaceuticals for Human

7   Use;

8   (C) activities that are subject to the protections provided in 21 C.F.R.

9   parts 50 (FDA clinical investigations protection of human subjects) and 56

10   (FDA clinical investigations institutional review boards); or

11   (D) research conducted in accordance with the requirements set forth

12   in subdivisions (A) through (C) of this subdivision (a)(4) or otherwise in

13   accordance with applicable law;

14   (5) patient identifying information that is collected and processed in

15   accordance with 42 C.F.R. part 2 (confidentiality of substance use disorder

16   patient records);

17   (6) patient safety work product that is created for purposes of improving

18   patient safety under 42 C.F.R. part 3 (patient safety organizations and patient

19   safety work product);

1   (7) information or documents created for the purposes of the Healthcare

2   Quality Improvement Act of 1986, 42 U.S.C. § 11101–11152, and regulations

3   adopted to implement that act;

4   (8) information that originates from, that is intermingled so as to be

5   indistinguishable from, or that is treated in the same manner as information

6   described in subdivisions (2)–(7) of this subsection that a covered entity,

7   business associate, or a qualified service organization program creates,

8   collects, processes, uses, or maintains in the same manner as is required under

9   the laws, regulations, and guidelines described in subdivisions (2)–(7) of this

10   subsection;

11   (9) information processed or maintained solely in connection with, and

12   for the purpose of, enabling:

13   (A) an individual's employment or application for employment;

14   (B) an individual's ownership of, or function as a director or officer

15   of, a business entity;

16   (C) an individual's contractual relationship with a business entity;

17   (D) an individual's receipt of benefits from an employer, including

18   benefits for the individual's dependents or beneficiaries; or

19   (E) notice of an emergency to persons that an individual specifies;

20   (10) any activity that involves collecting, maintaining, disclosing,

21   selling, communicating, or using information for the purpose of evaluating a

1   consumer's creditworthiness, credit standing, credit capacity, character,

2   general reputation, personal characteristics, or mode of living if done strictly in

3   accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C.

4   § 1681–1681x, as may be amended, by:

5   (A) a consumer reporting agency;

6   (B) a person who furnishes information to a consumer reporting

7   agency under 15 U.S.C. § 1681s-2 (responsibilities of furnishers of

8   information to consumer reporting agencies); or

9   (C) a person who uses a consumer report as provided in 15 U.S.C.

10   § 1681b(a)(3) (permissible purposes of consumer reports);

11   (11) information collected, processed, sold, or disclosed under and in

12   accordance with the following laws and regulations:

13   (A) the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721–

14   2725;

15   (B) the Airline Deregulation Act, Pub. L. No. 95-504, only to the

16   extent that an air carrier collects information related to prices, routes, or

17   services, and only to the extent that the provisions of the Airline Deregulation

18   Act preempt this chapter;

19   (C) the Farm Credit Act, Pub. L. No. 92-181, as may be amended; or

20   (D) federal policy under 21 U.S.C. § 830 (regulation of listed

21   chemicals and certain machines);

1   (12) nonpublic personal information that is processed by a financial

2   institution or data subject to the Gramm-Leach-Bliley Act, Pub. L. No. 106-

3   102, and regulations adopted to implement that act;

4   (13) information that originates from, or is intermingled so as to be

5   indistinguishable from, information described in subdivision (12) of this

6   subsection and that a controller or processor collects, processes, uses, or

7   maintains in the same manner as is required under the law and regulations

8   specified in subdivision (12) of this subsection;

9   (14) a financial institution, credit union, independent trust company,

10   broker-dealer, or investment adviser or a financial institution's, credit union's,

11   independent trust company's, broker-dealer's, or investment adviser's affiliate

12   or subsidiary that is only and directly engaged in financial activities, as

13   described in 12 U.S.C. § 1843(k);

14   (15) a person regulated pursuant to part 3 of Title 8 (chapters 101–165)

15   other than a person that, alone or in combination with another person,

16   establishes and maintains a self-insurance program and that does not otherwise

17   engage in the business of entering into policies of insurance;

18   (16) a third-party administrator, as that term is defined in the Third Party

19   Administrator Rule adopted pursuant to 18 V.S.A. § 9417;

20   (17) a nonprofit organization that is established to detect and prevent

21   fraudulent acts in connection with insurance;

1   (18) a public service company subject to the rules and orders of the

2   Vermont Public Utility Commission regarding data sharing and service quality;

3   (19) an educational institution subject to the Family Educational Rights

4   and Privacy Act, 20 U.S.C. § 1232g, and regulations adopted to implement that

5   act;

6   (20) personal data of a victim or witness of child abuse, domestic

7   violence, human trafficking, sexual assault, violent felony, or stalking that a

8   victim services organization collects, processes, or maintains in the course of

9   its operation;

10   (21) personal data of health care service volunteers held by nonprofit

11   organizations to facilitate provision of health care services; or

12   (22) noncommercial activity of:

13   (A) a publisher, editor, reporter, or other person who is connected

14   with or employed by a newspaper, magazine, periodical, newsletter, pamphlet,

15   report, or other publication in general circulation;

16   (B) a radio or television station that holds a license issued by the

17   Federal Communications Commission;

18   (C) a nonprofit organization that provides programming to radio or

19   television networks; or

20   (D) an entity that provides an information service, including a press

21   association or wire service.

1   (b) Controllers, processors, and consumer health data controllers that

2   comply with the verifiable parental consent requirements of COPPA shall be

3   deemed compliant with any obligation to obtain parental consent pursuant to

4   this chapter, including pursuant to section 2420 of this title.

5   § 2418. CONSUMER PERSONAL DATA RIGHTS

6   (a) A consumer shall have the right to:

7   (1) confirm whether or not a controller is processing the consumer's

8   personal data and access the personal data, unless the confirmation or access

9   would require the controller to reveal a trade secret;

10   (2) obtain from a controller a list of third parties, other than individuals,

11   to which the controller has transferred, at the controller's election, either the

12   consumer's personal data or any personal data;

13   (3) correct inaccuracies in the consumer's personal data, taking into

14   account the nature of the personal data and the purposes of the processing of

15   the consumer's personal data;

16   (4) delete personal data provided by, or obtained about, the consumer;

17   (5) obtain a copy of the consumer's personal data processed by the

18   controller, in a portable and, to the extent technically feasible, readily usable

19   format that allows the consumer to transmit the data to another controller

20   without hindrance, where the processing is carried out by automated means,

21   provided such controller shall not be required to reveal any trade secret; and

1   (6) opt out of the processing of the personal data for purposes of:

2   (A) targeted advertising;

3   (B) the sale of personal data; or

4   (C) profiling in furtherance of solely automated decisions that

5   produce legal or similarly significant effects concerning the consumer.

6   (b)(1) A consumer may exercise rights under this section by submitting a

7   request to a controller using the method that the controller specifies in the

8   privacy notice under section 2419 of this title.

9   (2) A controller shall not require a consumer to create an account for the

10   purpose described in subdivision (1) of this subsection, but the controller may

11   require the consumer to use an account the consumer previously created.

12   (3) A parent or legal guardian may exercise rights under this section on

13   behalf of the parent's child or on behalf of a child for whom the guardian has

14   legal responsibility. A guardian or conservator may exercise the rights under

15   this section on behalf of a consumer that is subject to a guardianship,

16   conservatorship, or other protective arrangement.

17   (4)(A) A consumer may designate another person to act on the

18   consumer's behalf as the consumer's authorized agent for the purpose of

19   exercising the consumer's rights under subdivision (a)(4) or (a)(6) of this

20   section.

1   (B) The consumer may designate an authorized agent by means of an

2   internet link, browser setting, browser extension, global device setting, or other

3   technology that enables the consumer to exercise the consumer's rights under

4   subdivision (a)(4) or (a)(6) of this section.

5   (c) Except as otherwise provided in this chapter, a controller shall comply

6   with a request by a consumer to exercise the consumer rights authorized

7   pursuant to this chapter as follows:

8   (1)(A) A controller shall respond to the consumer without undue delay,

9   but not later than 60 days after receipt of the request.

10   (B) The controller may extend the response period by 45 additional

11   days when reasonably necessary, considering the complexity and number of

12   the consumer's requests, provided the controller informs the consumer of the

13   extension within the initial 60-day response period and of the reason for the

14   extension.

15   (2) If a controller declines to take action regarding the consumer's

16   request, the controller shall inform the consumer without undue delay, but not

17   later than 45 days after receipt of the request, of the justification for declining

18   to take action and instructions for how to appeal the decision.

19   (3)(A) Information provided in response to a consumer request shall be

20   provided by a controller, free of charge, once per consumer during any 12-

21   month period.

1   (B) If requests from a consumer are manifestly unfounded, excessive,

2   or repetitive, the controller may charge the consumer a reasonable fee to cover

3   the administrative costs of complying with the request or decline to act on the

4   request.

5   (C) The controller bears the burden of demonstrating the manifestly

6   unfounded, excessive, or repetitive nature of the request.

7   (4)(A) If a controller is unable to authenticate a request to exercise any

8   of the rights afforded under subdivisions (a)(1)–(5) of this section using

9   commercially reasonable efforts, the controller shall not be required to comply

10   with a request to initiate an action pursuant to this section and shall provide

11   notice to the consumer that the controller is unable to authenticate the request

12   to exercise the right or rights until the consumer provides additional

13   information reasonably necessary to authenticate the consumer and the

14   consumer's request to exercise the right or rights.

15   (B) A controller shall not be required to authenticate an opt-out

16   request, but a controller may deny an opt-out request if the controller has a

17   good faith, reasonable, and documented belief that the request is fraudulent.

18   (C) If a controller denies an opt-out request because the controller

19   believes the request is fraudulent, the controller shall send a notice to the

20   person who made the request disclosing that the controller believes the request

1   is fraudulent, why the controller believes the request is fraudulent, and that the

2   controller shall not comply with the request.

3   (5) A controller that has obtained personal data about a consumer from a

4   source other than the consumer shall be deemed in compliance with a

5   consumer's request to delete the data pursuant to subdivision (a)(4) of this

6   section by:

7   (A) retaining a record of the deletion request and the minimum data

8   necessary for the purpose of ensuring the consumer's personal data remains

9   deleted from the controller's records and not using the retained data for any

10   other purpose pursuant to the provisions of this chapter; or

11   (B) opting the consumer out of the processing of the personal data for

12   any purpose except for those exempted pursuant to the provisions of this

13   chapter.

14   (6) A controller may not condition the exercise of a right under this

15   section through:

16   (A) the use of any false, fictitious, fraudulent, or materially

17   misleading statement or representation; or

18   (B) the employment of any dark pattern.

19   (d) A controller shall establish a process by means of which a consumer

20   may appeal the controller's refusal to take action on a request under

21   subsection (b) of this section. The controller's process must:

1   (1) Allow a reasonable period of time after the consumer receives the

2   controller's refusal within which to appeal.

3   (2) Be conspicuously available to the consumer.

4   (3) Be similar to the manner in which a consumer must submit a request

5   under subsection (b) of this section.

6   (4) Require the controller to approve or deny the appeal within 45 days

7   after the date on which the controller received the appeal and to notify the

8   consumer in writing of the controller's decision and the reasons for the

9   decision. If the controller denies the appeal, the notice must provide or specify

10   information that enables the consumer to contact the Attorney General to

11   submit a complaint.

12   § 2419. DUTIES OF CONTROLLERS

13   (a) A controller shall:

14   (1) specify in the privacy notice described in subsection (d) of this

15   section the express purposes for which the controller is collecting and

16   processing personal data;

17   (2) process personal data only:

18   (A) as reasonably necessary and proportionate to achieve a disclosed

19   purpose for which the personal data was collected, consistent with the

20   reasonable expectations of the consumer whose personal data is being

21   processed;

1   (B) for another disclosed purpose that is compatible with the context

2   in which the personal data was collected; or

3   (C) for a further disclosed purpose if the controller obtains the

4   consumer's consent;

5   (3) establish, implement, and maintain reasonable administrative,

6   technical, and physical data security practices to protect the confidentiality,

7   integrity, and accessibility of personal data appropriate to the volume and

8   nature of the personal data at issue; and

9   (4) provide an effective mechanism for a consumer to revoke consent to

10   the controller's processing of the consumer's personal data that is at least as

11   easy as the mechanism by which the consumer provided the consumer's

12   consent and, upon revocation of the consent, cease to process the data as soon

13   as practicable, but not later than 60 days after receiving the request.

14   (b) A controller shall not:

15   (1) process personal data beyond what is reasonably necessary and

16   proportionate to the processing purpose;

17   (2) process sensitive data about a consumer without first obtaining the

18   consumer's consent or, if the controller knows the consumer is a child, without

19   processing the sensitive data in accordance with COPPA;

20   (3)(A) except as provided in subdivision (B) of this subdivision (3),

21   process a consumer's personal data in a manner that discriminates against

1   individuals or otherwise makes unavailable the equal enjoyment of goods or

2   services on the basis of an individual's actual or perceived race, color, sex,

3   sexual orientation or gender identity, physical or mental disability, religion,

4   ancestry, or national origin;

5   (B) subdivision (A) of this subdivision (3) shall not apply to:

6   (i) a private establishment, as that term is used in 42 U.S.C.

7   § 2000a(e) (prohibition against discrimination or segregation in places of

8   public accommodation);

9   (ii) processing for the purpose of a controller's or processor's self-

10   testing to prevent or mitigate unlawful discrimination; or

11   (iii) processing for the purpose of diversifying an applicant,

12   participant, or consumer pool.

13   (4) process a consumer's personal data for the purposes of targeted

14   advertising, of profiling the consumer in furtherance of decisions that produce

15   legal or similarly significant effects concerning the consumer, or of selling the

16   consumer's personal data without the consumer's consent if the controller

17   knows that the consumer is at least 13 years of age and not older than 16 years

18   of age; or

19   (5) discriminate or retaliate against a consumer who exercises a right

20   provided to the consumer under this chapter or refuses to consent to the

1   collection or processing of personal data for a separate product or service,

2   including by:

3   (A) denying goods or services;

4   (B) charging different prices or rates for goods or services; or

5   (C) providing a different level of quality or selection of goods or

6   services to the consumer.

7   (c) Subsections (a) and (b) of this section shall not be construed to:

8   (1) require a controller to provide a good or service that requires

9   personal data from a consumer that the controller does not collect or maintain;

10   or

11   (2) prohibit a controller from offering a different price, rate, level of

12   quality, or selection of goods or services to a consumer, including an offer for

13   no fee or charge, in connection with a consumer's voluntary participation in a

14   financial incentive program, such as a bona fide loyalty, rewards, premium

15   features, discount, or club card program.

16   (d)(1) A controller shall provide to consumers a reasonably accessible,

17   clear, and meaningful privacy notice that:

18   (A) lists the categories of personal data, including the categories of

19   sensitive data, that the controller processes;

20   (B) describes the controller's purposes for processing the personal

21   data;

1   (C) describes how a consumer may exercise the consumer's rights

2   under this chapter, including how a consumer may appeal a controller's denial

3   of a consumer's request under section 2418 of this title;

4   (D) lists all categories of personal data, including the categories of

5   sensitive data, that the controller shares with third parties;

6   (E) describes all categories of third parties with which the controller

7   shares personal data at a level of detail that enables the consumer to understand

8   what type of entity each third party is and, to the extent possible, how each

9   third party may process personal data;

10   (F) specifies an e-mail address or other online method by which a

11   consumer can contact the controller that the controller actively monitors;

12   (G) identifies the controller, including any business name under

13   which the controller registered with the Secretary of State and any assumed

14   business name that the controller uses in this State;

15   (H) provides a clear and conspicuous description of any processing of

16   personal data in which the controller engages for the purposes of targeted

17   advertising, sale of personal data to third parties, or profiling the consumer in

18   furtherance of decisions that produce legal or similarly significant effects

19   concerning the consumer, and a procedure by which the consumer may opt out

20   of this type of processing; and

1   (I) describes the method or methods the controller has established for

2   a consumer to submit a request under subdivision 2418(b)(1) of this title.

3   (2) The privacy notice shall adhere to the accessibility and usability

4   guidelines recommended under 42 U.S.C. chapter 126 (the Americans with

5   Disabilities Act) and 29 U.S.C. 794d (section 508 of the Rehabilitation Act of

6   1973), including ensuring readability for individuals with disabilities across

7   various screen resolutions and devices and employing design practices that

8   facilitate easy comprehension and navigation for all users.

9   (e) The method or methods under subdivision (d)(1)(I) of this section for

10   submitting a consumer's request to a controller must:

11   (1) take into account the ways in which consumers normally interact

12   with the controller, the need for security and reliability in communications

13   related to the request, and the controller's ability to authenticate the identity of

14   the consumer that makes the request;

15   (2) provide a clear and conspicuous link to a website where the

16   consumer or an authorized agent may opt out from a controller's processing of

17   the consumer's personal data pursuant to subdivision 2418(a)(6) of this title or,

18   solely if the controller does not have a capacity needed for linking to a

19   webpage, provide another method the consumer can use to opt out; and

20   (3) allow a consumer or authorized agent to send a signal to the

21   controller that indicates the consumer's preference to opt out of the sale of

1   personal data or targeted advertising pursuant to subdivision 2418(a)(6) of this

2   title by means of a platform, technology, or mechanism that:

3   (A) does not unfairly disadvantage another controller;

4   (B) does not use a default setting but instead requires the consumer or

5   authorized agent to make an affirmative, voluntary, and unambiguous choice to

6   opt out;

7   (C) is consumer friendly and easy for an average consumer to use;

8   (D) is as consistent as possible with similar platforms, technologies,

9   or mechanisms required under federal or state laws or regulations; and

10   (E) enables the controller to reasonably determine whether the

11   consumer has made a legitimate request pursuant to subsection 2418(b) of this

12   title to opt out pursuant to subdivision 2418(a)(6) of this title.

13   (f) If a consumer or authorized agent uses a method under subdivision

14   (d)(1)(I) of this section to opt out of a controller's processing of the

15   consumer's personal data pursuant to subdivision 2418(a)(6) of this title and

16   the decision conflicts with a consumer's voluntary participation in a bona fide

17   reward, club card, or loyalty program or a program that provides premium

18   features or discounts in return for the consumer's consent to the controller's

19   processing of the consumer's personal data, the controller may either comply

20   with the request to opt out or notify the consumer of the conflict and ask the

21   consumer to affirm that the consumer intends to withdraw from the bona fide

1   reward, club card, or loyalty program or the program that provides premium

2   features or discounts. If the consumer affirms that the consumer intends to

3   withdraw, the controller shall comply with the request to opt out.

4   § 2420. DUTIES OF CONTROLLERS TO MINORS

5   (a)(1) A controller that offers any online service, product, or feature to a

6   consumer whom the controller knows is a minor shall use reasonable care to

7   avoid any heightened risk of harm to minors caused by the online service,

8   product, or feature.

9   (2) In any action brought pursuant to section 2425 of this title, there is a

10   rebuttable presumption that a controller used reasonable care as required under

11   this section if the controller complied with this section.

12   (b) Unless a controller has obtained consent in accordance with subsection

13   (c) of this section, a controller that offers any online service, product, or

14   feature to a consumer whom the controller knows is a minor shall not:

15   (1) process a minor's personal data for the purposes of:

16   (A) targeted advertising;

17   (B) the sale of personal data; or

18   (C) profiling in furtherance of any solely automated decisions that

19   produce legal or similarly significant effects concerning the consumer;

20   (2) process a minor's personal data for any purpose other than:

1   (A) the processing purpose that the controller disclosed at the time

2   the controller collected the minor's personal data; or

3   (B) a processing purpose that is reasonably necessary for, and

4   compatible with, the processing purpose that the controller disclosed at the

5   time the controller collected the minor's personal data; or

6   (3) process a minor's personal data for longer than is reasonably

7   necessary to provide the online service, product, or feature;

8   (4) use any system design feature, except for a service or application that

9   is used by and under the direction of an educational entity, to significantly

10   increase, sustain, or extend a minor's use of the online service, product, or

11   feature; or

12   (5) collect a minor's precise geolocation data unless:

13   (A) the minor's precise geolocation data is reasonably necessary for

14   the controller to provide the online service, product, or feature;

15   (B) the controller only collects the minor's precise geolocation data

16   for the time necessary to provide the online service, product, or feature; and

17   (C) the controller provides to the minor a signal indicating that the

18   controller is collecting the minor's precise geolocation data and makes the

19   signal available to the minor for the entire duration of the collection of the

20   minor's precise geolocation data.

1   (c) A controller shall not engage in the activities described in subsection (b)

2   of this section unless the controller obtains:

3   (1) the minor's consent; or

4   (2) if the minor is a child, the consent of the minor's parent or legal

5   guardian.

6   (d) A controller that offers any online service, product, or feature to a

7   consumer whom that controller knows is a minor shall not:

8   (1) employ any dark pattern; or

9   (2) except as provided in subsection (e) of this section, offer any direct

10   messaging apparatus for use by a minor without providing readily accessible

11   and easy-to-use safeguards to limit the ability of an adult to send unsolicited

12   communications to the minor with whom the adult is not connected.

13   (e) Subdivision (d)(2) of this section does not apply to an online service,

14   product, or feature of which the predominant or exclusive function is:

15   (1) e-mail; or

16   (2) direct messaging consisting of text, photographs, or videos that are

17   sent between devices by electronic means, where messages are:

18   (A) shared between the sender and the recipient;

19   (B) only visible to the sender and the recipient; and

20   (C) not posted publicly.

21   § 2421. DUTIES OF PROCESSORS

1   (a) A processor shall adhere to a controller's instructions and shall assist

2   the controller in meeting the controller's obligations under this chapter. In

3   assisting the controller, the processor must:

4   (1) enable the controller to respond to requests from consumers pursuant

5   to subsection 2418(b) of this title by means that:

6   (A) take into account how the processor processes personal data and

7   the information available to the processor; and

8   (B) use appropriate technical and organizational measures to the

9   extent reasonably practicable; and

10   (2) adopt administrative, technical, and physical safeguards that are

11   reasonably designed to protect the security and confidentiality of the personal

12   data the processor processes, taking into account how the processor processes

13   the personal data and the information available to the processor.

14   (b) Processing by a processor must be governed by a contract between the

15   controller and the processor. The contract must:

16   (1) be valid and binding on both parties;

17   (2) set forth clear instructions for processing data, the nature and

18   purpose of the processing, the type of data that is subject to processing, and the

19   duration of the processing;

20   (3) specify the rights and obligations of both parties with respect to the

21   subject matter of the contract;

1   (4) ensure that each person that processes personal data is subject to a

2   duty of confidentiality with respect to the personal data;

3   (5) require the processor to delete the personal data or return the

4   personal data to the controller at the controller's direction or at the end of the

5   provision of services, unless a law requires the processor to retain the personal

6   data;

7   (6) require the processor to make available to the controller, at the

8   controller's request, all information the controller needs to verify that the

9   processor has complied with all obligations the processor has under this

10 chapter;

11   (7) require the processor to enter into a subcontract with a person the

12 processor engages to assist with processing personal data on the controller's

13 behalf and in the subcontract require the subcontractor to meet the processor's

14 obligations concerning personal data; and

15   (8)(A) allow the controller, the controller's designee, or a qualified and

16 independent person the processor engages, in accordance with an appropriate

17 and accepted control standard, framework, or procedure, to assess the

18 processor's policies and technical and organizational measures for complying

19 with the processor's obligations under this chapter;

20   (B) require the processor to cooperate with the assessment; and

1   (C) at the controller's request, report the results of the assessment to

2   the controller.

3   (c) This section does not relieve a controller or processor from any liability

4   that accrues under this chapter as a result of the controller's or processor's

5   actions in processing personal data.

6   (d)(1) For purposes of determining obligations under this chapter, a person

7   is a controller with respect to processing a set of personal data and is subject to

8   an action under section 2425 of this title to punish a violation of this chapter, if

9   the person:

10   (A) does not adhere to a controller's instructions to process the

11   personal data; or

12   (B) begins at any point to determine the purposes and means for

13   processing the personal data, alone or in concert with another person.

14   (2) A determination under this subsection is a fact-based determination

15   that must take account of the context in which a set of personal data is

16   processed.

17   (3) A processor that adheres to a controller's instructions with respect to

18   a specific processing of personal data remains a processor.

1   § 2422. DUTIES OF PROCESSORS TO MINORS

2   (a) A processor shall adhere to the instructions of a controller and shall

3   assist the controller in meeting the controller's obligations under section 2420

4   of this title, taking into account:

5   (1) the nature of the processing;

6   (2) the information available to the processor by appropriate technical

7   and organizational measures; and

8   (3) whether the assistance is reasonably practicable and necessary to

9   assist the controller in meeting its obligations.

10   (b) A contract between a controller and a processor must satisfy the

11   requirements in subsection 2421(b) of this title.

12   (c) Nothing in this section shall be construed to relieve a controller or

13   processor from the liabilities imposed on the controller or processor by virtue

14   of the controller's or processor's role in the processing relationship as

15   described in section 2420 of this title.

16   (d) Determining whether a person is acting as a controller or processor with

17   respect to a specific processing of data is a fact-based determination that

18   depends upon the context in which personal data is to be processed. A person

19   that is not limited in the person's processing of personal data pursuant to a

20   controller's instructions, or that fails to adhere to the instructions, is a

21   controller and not a processor with respect to a specific processing of data. A

1   processor that continues to adhere to a controller's instructions with respect to

2   a specific processing of personal data remains a processor. If a processor

3   begins, alone or jointly with others, determining the purposes and means of the

4   processing of personal data, the processor is a controller with respect to the

5   processing and may be subject to an enforcement action under section 2425 of

6   this title.

7   § 2423. DE-IDENTIFIED OR PSEUDONYMOUS DATA

8   (a) A controller in possession of de-identified data shall:

9   (1) take reasonable measures to ensure that the data cannot be used to

10   re-identify an identified or identifiable individual or be associated with an

11   individual or device that identifies or is linked or reasonably linkable to an

12   individual or household;

13   (2) publicly commit to maintaining and using de-identified data without

14   attempting to re-identify the data; and

15   (3) contractually obligate any recipients of the de-identified data to

16   comply with the provisions of this chapter.

17   (b) This section does not prohibit a controller from attempting to re-

18   identify de-identified data solely for the purpose of testing the controller's

19   methods for de-identifying data.

20   (c) This chapter shall not be construed to require a controller or processor

21   to:

1   (1) re-identify de-identified data; or

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

3   any data or technology, in order to associate a consumer with personal data in

4   order to authenticate the consumer's request under subsection 2418(b) of this

5   title; or

6   (3) comply with an authenticated consumer rights request if the

7   controller:

8   (A) is not reasonably capable of associating the request with the

9   personal data or it would be unreasonably burdensome for the controller to

10   associate the request with the personal data;

11   (B) does not use the personal data to recognize or respond to the

12   specific consumer who is the subject of the personal data or associate the

13   personal data with other personal data about the same specific consumer; and

14   (C) does not sell or otherwise voluntarily disclose the personal data

15   to any third party, except as otherwise permitted in this section.

16   (d) The rights afforded under subdivisions 2418(a)(1)–(5) of this title shall

17   not apply to pseudonymous data in cases where the controller is able to

18   demonstrate that any information necessary to identify the consumer is kept

19   separately and is subject to effective technical and organizational controls that

20   prevent the controller from accessing the information.

1   (e) A controller that discloses or transfers pseudonymous data or de-

2   identified data shall exercise reasonable oversight to monitor compliance with

3   any contractual commitments to which the pseudonymous data or de-identified

4   data is subject and shall take appropriate steps to address any breaches of those

5   contractual commitments.

6   § 2424. CONSTRUCTION OF DUTIES OF CONTROLLERS AND

7   PROCESSORS

8   (a) This chapter shall not be construed to restrict a controller's, processor's,

9   or consumer health data controller's ability to:

10   (1) comply with federal, state, or municipal laws, ordinances, or

11   regulations;

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

13   subpoena, or summons by federal, state, municipal, or other governmental

14   authorities;

15   (3) cooperate with law enforcement agencies concerning conduct or

16   activity that the controller, processor, or consumer health data controller

17   reasonably and in good faith believes may violate federal, state, or municipal

18   laws, ordinances, or regulations;

19   (4) carry out obligations under a contract under subsection 2421(b) of

20   this title for a federal, State, tribal, or local government entity;

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

1   (6) provide a product or service specifically requested by the consumer

2   to whom the personal data pertains;

3   (7) perform under a contract to which a consumer is a party, including

4   fulfilling the terms of a written warranty;

5   (8) take steps at the request of a consumer prior to entering into a

6   contract;

7   (9) take immediate steps to protect an interest that is essential for the life

8   or physical safety of the consumer or another individual, and where the

9   processing cannot be manifestly based on another legal basis;

10   (10) prevent, detect, protect against, or respond to a network security or

11   physical security incident, including an intrusion or trespass, medical alert, or

12   fire alarm;

13   (11) prevent, detect, protect against, or respond to identity theft, fraud,

14   harassment, malicious or deceptive activity, or any criminal activity targeted at

15   or involving the controller or processor or its services, preserve the integrity or

16   security of systems, or investigate, report, or prosecute those responsible for

17   the action;

18   (12) assist another controller, processor, consumer health data

19   controller, or third party with any of the obligations under this chapter; or

1   (13) process personal data for reasons of public interest in the area of

2   public health, community health, or population health, but solely to the extent

3   that the processing is:

4   (A) subject to suitable and specific measures to safeguard the rights

5   of the consumer whose personal data is being processed; and

6   (B) under the responsibility of a professional subject to

7   confidentiality obligations under federal, state, or local law.

8   (b) The obligations imposed on controllers, processors, or consumer health

9   data controllers under this chapter shall not restrict a controller's, processor's,

10   or consumer health data controller's ability to collect, use, or retain data for

11   internal use to:

12   (1) conduct internal research to develop, improve, or repair products,

13   services, or technology;

14   (2) effectuate a product recall; or

15   (3) identify and repair technical errors that impair existing or intended

16   functionality.

17   (c)(1) The obligations imposed on controllers, processors, or consumer

18   health data controllers under this chapter shall not apply where compliance by

19   the controller, processor, or consumer health data controller with this chapter

20   would violate an evidentiary privilege under the laws of this State.

1   (2) This chapter shall not be construed to prevent a controller, processor,

2   or consumer health data controller from providing personal data concerning a

3   consumer to a person covered by an evidentiary privilege under the laws of the

4   State as part of a privileged communication.

5   (d)(1) A controller, processor, or consumer health data controller that

6   discloses personal data to a processor or third-party controller pursuant to this

7   chapter shall not be deemed to have violated this chapter if the processor or

8   third-party controller that receives and processes the personal data violates this

9   chapter, provided, at the time the disclosing controller, processor, or consumer

10   health data controller disclosed the personal data, the disclosing controller,

11   processor, or consumer health data controller did not have actual knowledge

12   that the receiving processor or third-party controller would violate this chapter.

13   (2) A third-party controller or processor receiving personal data from a

14   controller, processor, or consumer health data controller in compliance with

15   this chapter is not in violation of this chapter for the transgressions of the

16   controller, processor, or consumer health data controller from which the third-

17   party controller or processor receives the personal data.

18   (e) This chapter shall not be construed to:

19   (1) impose any obligation on a controller, processor, or consumer health

20   data controller that adversely affects the rights or freedoms of any person,

21   including the rights of any person:

1   (A) to freedom of speech or freedom of the press guaranteed in the

2   First Amendment to the U.S. Constitution; or

3   (B) under 12 V.S.A. § 1615; or

4   (2) apply to any person's processing of personal data in the course of the

5   person's purely personal or household activities.

6   (f)(1) Personal data processed by a controller or consumer health data

7   controller pursuant to this section may be processed to the extent that the

8   processing is:

9   (A) reasonably necessary and proportionate to the purposes listed in

10   this section; and

11   (B) adequate, relevant, and limited to what is necessary in relation to

12   the specific purposes listed in this section.

13   (2)(A) Personal data collected, used, or retained pursuant to subsection

14   (b) of this section shall, where applicable, take into account the nature and

15   purpose or purposes of the collection, use, or retention.

16   (B) Personal data collected, used, or retained pursuant to subsection

17   (b) of this section shall be subject to reasonable administrative, technical, and

18   physical measures to protect the confidentiality, integrity, and accessibility of

19   the personal data and to reduce reasonably foreseeable risks of harm to

20   consumers relating to the collection, use, or retention of personal data.

1   (g) If a controller or consumer health data controller processes personal

2   data pursuant to an exemption in this section, the controller or consumer health

3   data controller bears the burden of demonstrating that the processing qualifies

4   for the exemption and complies with the requirements in subsection (f) of this

5   section.

6   (h) Processing personal data for the purposes expressly identified in this

7   section shall not solely make a legal entity a controller or consumer health data

8   controller with respect to the processing.

9   § 2425. ENFORCEMENT; ATTORNEY GENERAL'S POWERS

10   (a) The Attorney General shall have exclusive authority to enforce

11   violations of this chapter.

12   (b)(1) The Attorney General may, prior to initiating any action for a

13   violation of any provision of this chapter, issue a notice of violation to the

14   controller or consumer health data controller if the Attorney General

15   determines that a cure is possible.

16   (2) The Attorney General may, in determining whether to grant a

17   controller, processor, or consumer health data controller the opportunity to

18   cure an alleged violation described in subdivision (1) of this subsection,

19   consider:

20   (A) the number of violations;

1   (B) the size and complexity of the controller, processor, or consumer

2   health data controller;

3   (C) the nature and extent of the controller's, processor's, or consumer

4   health data controller's processing activities;

5   (D) the substantial likelihood of injury to the public;

6   (E) the safety of persons or property;

7   (F) whether the alleged violation was likely caused by human or

8   technical error; and

9   (G) the sensitivity of the data.

10   (c) Annually, on or before February 1, the Attorney General shall submit a

11   report to the General Assembly disclosing:

12   (1) the number of notices of violation the Attorney General has issued;

13   (2) the nature of each violation;

14   (3) the number of violations that were cured during the available cure

15   period; and

16   (4) any other matter the Attorney General deems relevant for the

17   purposes of the report.

18   (d) This chapter shall not be construed as providing the basis for, or be

19   subject to, a private right of action for violations of this chapter or any other

20   law.

1   (e) A violation of the requirements of this chapter shall constitute an unfair

2   and deceptive act in commerce in violation of section 2453 of this title and

3   shall be enforced solely by the Attorney General, provided that a consumer

4   private right of action under subsection 2461(b) of this title shall not apply to

5   the violation.

6   § 2426. CONFIDENTIALITY OF CONSUMER HEALTH DATA

7   Except as provided in subsections 2417(a) and (b) of this title and section

8   2424 of this title, no person shall:

9   (1) provide any employee or contractor with access to consumer health

10   data unless the employee or contractor is subject to a contractual or statutory

11   duty of confidentiality;

12   (2) provide any processor with access to consumer health data unless the

13   person and processor comply with section 2421 of this title;

14   (3) use a geofence to establish a virtual boundary that is within 1,850

15   feet of any health care facility, mental health facility, or reproductive or sexual

16   health facility for the purpose of identifying, tracking, collecting data from, or

17   sending any notification to a consumer regarding the consumer's consumer

18   health data; or

19   (4) sell or offer to sell consumer health data without first obtaining the

20   consumer's consent.

1   Sec. 2. 3 V.S.A. § 5023 is amended to read:

2   § 5023. ARTIFICIAL INTELLIGENCE AND DATA PRIVACY

3   ADVISORY COUNCIL

4   (a)(1) Advisory Council. There is established the Artificial Intelligence

5   and Data Privacy Advisory Council to:

6   (A) provide advice and counsel to the Director of the Division of

7   Artificial Intelligence with regard to on the Division's responsibilities to

8   review all aspects of artificial intelligence systems developed, employed, or

9   procured in State government.;

10   (B) The Council, in consultation with the Director of the Division,

11   shall also engage in public outreach and education on artificial intelligence;

12   (C) provide advice and counsel to the Attorney General in carrying

13   out the Attorney General's enforcement responsibilities under the Vermont

14   Data Privacy Act; and

15   (D) develop policy recommendations for improving data privacy in

16   Vermont, including recommendations for implementing a private right of

17   action and developing education and outreach on the Vermont Data Privacy

18   Act.

19   (2) The Advisory Council shall have the authority to establish

20   subcommittees to carry out the purposes of subdivision (D) of subdivision (1).

21   (b) Members.

1   (1) Members. The Advisory Council shall be composed of the

2   following members:

3   (A) the Secretary of Digital Services or designee;

4   (B) the Secretary of Commerce and Community Development or

5   designee;

6   (C) the Commissioner of Public Safety or designee;

7   (D) the Executive Director of the American Civil Liberties Union of

8   Vermont or designee;

9   (E) one member who is an expert in constitutional and legal rights,

10   appointed by the Chief Justice of the Supreme Court;

11   (F) one member with experience in the field of ethics and human

12   rights, appointed by the Governor;

13   (G) one member who is an academic at a postsecondary institute,

14   appointed by the Vermont Academy of Science and Engineering;

15   (H) the Commissioner of Health or designee;

16   (I) the Executive Director of Racial Equity or designee; ~~and~~

17   (J) the Attorney General or designee;

18   (K) one member representing Vermont small businesses, appointed

19   by the Speaker of the House; and

20   (L) one member who is an expert in data privacy, appointed by the

21   Committee on Committees.

1   (2) Chair. Members of the Advisory Council shall elect by majority

2   vote the Chair of the Advisory Council. Members of the Advisory Council

3   shall be appointed on or before August 1, 2022 in order to prepare as they

4   deem necessary for the establishment of the Advisory Council, including the

5   election of the Chair of the Advisory Council, except that the member

6   representing Vermont small businesses and the member who is an expert in

7   data privacy shall be appointed on or before August 1, 2024.

8   (3) Qualifications. Members shall be drawn from diverse backgrounds

9   and, to the extent possible, have experience with artificial intelligence.

10   (c) Meetings. The Advisory Council shall meet at the call of the Chair as

11   follows:

12   (1) on or before January 31, 2024, not more than 12 times; and

13   (2) on or after February 1, 2024, not more than monthly.

14   (d) Quorum. A majority of members shall constitute a quorum of the

15   Advisory Council. Once a quorum has been established, the vote of a majority

16   of the members present at the time of the vote shall be an act of the Advisory

17   Council.

18   (e) Assistance. The Advisory Council shall have the administrative and

19   technical support of the Agency of Digital Services.

20   (f) Reimbursement. Members of the Advisory Council who are not

21   employees of the State of Vermont and who are not otherwise compensated or

1   reimbursed for their attendance shall be entitled to compensation and expenses

2   as provided in 32 V.S.A. § 1010.

3   (g) Consultation. ~~The~~ In its advice and counsel to the Director of the

4   Division of Artificial Intelligence, the Advisory Council shall consult with any

5   relevant national bodies on artificial intelligence, including the National

6   Artificial Intelligence Advisory Committee established by the Department of

7   Commerce, and its applicability to Vermont. In its advice and counsel to the

8   Attorney General, the Advisory Council shall consult with enforcement

9   authorities in states with comparable comprehensive data privacy regimes.

10   (h) Repeal. This section shall be repealed on June 30, 2027.

11   (i) Limitation. The advice and counsel of the Advisory Council shall not

12   limit the discretionary authority of the Attorney General to enforce the

13   Vermont Data Privacy Act.

14   Sec. 3. 9 V.S.A. chapter 62 is amended to read:

15   CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

16   Subchapter 1. General Provisions

17   § 2430. DEFINITIONS

18   As used in this chapter:

19   (1) "Biometric data" shall have the same meaning as in section 2415 of

20   this title.

1   (2)(A) "Brokered personal information" means one or more of the

2   following computerized data elements about a consumer, if categorized or

3   organized for dissemination to third parties:

4   (i) name;

5   (ii) address;

6   (iii) date of birth;

7   (iv) place of birth;

8   (v) mother's maiden name;

9   (vi) ~~unique biometric data generated from measurements or~~

10   ~~technical analysis of human body characteristics used by the owner or licensee~~

11   ~~of the data to identify or authenticate the consumer, such as a fingerprint, retina~~

12   ~~or iris image, or other unique physical representation or digital representation~~

13   ~~of~~ biometric data;

14   (vii) name or address of a member of the consumer's immediate

15   family or household;

16   (viii) Social Security number or other government-issued

17   identification number; or

18   (ix) other information that, alone or in combination with the other

19   information sold or licensed, would allow a reasonable person to identify the

20   consumer with reasonable certainty.

1   (B) "Brokered personal information" does not include publicly

2   available information ~~to the extent that it is related to a consumer's business or~~

3   ~~profession~~ as that term is defined in section 2415 of this title.

4   ~~(2)~~(3) "Business" means a controller, a consumer health data controller,

5   a processor, or a commercial entity, including a sole proprietorship,

6   partnership, corporation, association, limited liability company, or other group,

7   however organized and whether or not organized to operate at a profit,

8   including a financial institution organized, chartered, or holding a license or

9   authorization certificate under the laws of this State, any other state, the United

10   States, or any other country, or the parent, affiliate, or subsidiary of a financial

11   institution, but does not include the State, a State agency, any political

12   subdivision of the State, or a vendor acting solely on behalf of, and at the

13   direction of, the State.

14   ~~(3)~~(4) "Consumer" means an individual ~~residing in this State~~ who is a

15   resident of the State or an individual who is in the State at the time a data

16   broker collects the individual's data.

17   (5) "Consumer health data controller" has the same meaning as in

18   section 2415 of this title.

19   (6) "Controller" has the same meaning as in section 2415 of this title.

20   ~~(4)~~(7)(A) "Data broker" means a business, or unit or units of a business,

21   separately or together, that knowingly collects and sells or licenses to third

1   parties the brokered personal information of a consumer with whom the

2   business does not have a direct relationship.

3   (B) Examples of a direct relationship with a business include if the

4   consumer is a past or present:

5   (i) customer, client, subscriber, user, or registered user of the

6   business's goods or services;

7   (ii) employee, contractor, or agent of the business;

8   (iii) investor in the business; or

9   (iv) donor to the business.

10   (C) The following activities conducted by a business, and the

11   collection and sale or licensing of brokered personal information incidental to

12   conducting these activities, do not qualify the business as a data broker:

13   (i) developing or maintaining third-party e-commerce or

14   application platforms;

15   (ii) providing 411 directory assistance or directory information

16   services, including name, address, and telephone number, on behalf of or as a

17   function of a telecommunications carrier;

18   (iii) providing publicly available information related to a

19   consumer's business or profession; or

20   (iv) providing publicly available information via real-time or near-

21   real-time alert services for health or safety purposes.

1   (D) The phrase "sells or licenses" does not include:

2   (i) a one-time or occasional sale of assets of a business as part of a

3   transfer of control of those assets that is not part of the ordinary conduct of the

4   business; ~~or~~

5   (ii) a sale or license of data that is merely incidental to the

6   business; or

7   (iii) the disclosure of brokered personal information that a

8   consumer intentionally made available to the general public via a channel of

9   mass media and did not restrict to a specific audience.

10   ~~(5)~~(8)(A) "Data broker security breach" means an unauthorized

11   acquisition or a reasonable belief of an unauthorized acquisition of more than

12   one element of brokered personal information maintained by a data broker

13   when the brokered personal information is not encrypted, redacted, or

14   protected by another method that renders the information unreadable or

15   unusable by an unauthorized person.

16   (B) "Data broker security breach" does not include good faith but

17   unauthorized acquisition of brokered personal information by an employee or

18   agent of the data broker for a legitimate purpose of the data broker, provided

19   that the brokered personal information is not used for a purpose unrelated to

20   the data broker's business or subject to further unauthorized disclosure.

1   (C) In determining whether brokered personal information has been

2   acquired or is reasonably believed to have been acquired by a person without

3   valid authorization, a data broker may consider the following factors, among

4   others:

5   (i) indications that the brokered personal information is in the

6   physical possession and control of a person without valid authorization, such

7   as a lost or stolen computer or other device containing brokered personal

8   information;

9   (ii) indications that the brokered personal information has been

10   downloaded or copied;

11   (iii) indications that the brokered personal information was used

12   by an unauthorized person, such as fraudulent accounts opened or instances of

13   identity theft reported; or

14   (iv) that the brokered personal information has been made public.

15   (6)(9) "Data collector" means a person who, for any purpose, whether

16   by automated collection or otherwise, handles, collects, disseminates, or

17   otherwise deals with personally identifiable information, and includes the

18   State, State agencies, political subdivisions of the State, public and private

19   universities, privately and publicly held corporations, limited liability

20   companies, financial institutions, and retail operators.

1   (7)(10) "Encryption" means use of an algorithmic process to transform

2   data into a form in which the data is rendered unreadable or unusable without

3   use of a confidential process or key.

4   (8)(11) "License" means a grant of access to, or distribution of, data by

5   one person to another in exchange for consideration. A use of data for the sole

6   benefit of the data provider, where the data provider maintains control over the

7   use of the data, is not a license.

8   (9)(12) "Login credentials" means a consumer's user name or e-mail

9   address, in combination with a password or an answer to a security question,

10   that together permit access to an online account.

11   (10)(13)(A) "Personally identifiable information" means a consumer's

12   first name or first initial and last name in combination with one or more of the

13   following digital data elements, when the data elements are not encrypted,

14   redacted, or protected by another method that renders them unreadable or

15   unusable by unauthorized persons:

16   (i) a Social Security number;

17   (ii) a driver license or nondriver State identification card number,

18   individual taxpayer identification number, passport number, military

19   identification card number, or other identification number that originates from

20   a government identification document that is commonly used to verify identity

21   for a commercial transaction;

1   (iii) a financial account number or credit or debit card number, if

2   the number could be used without additional identifying information, access

3   codes, or passwords;

4   (iv) a password, personal identification number, or other access

5   code for a financial account;

6   (v) ~~unique biometric data generated from measurements or~~

7   ~~technical analysis of human body characteristics used by the owner or licensee~~

8   ~~of the data to identify or authenticate the consumer, such as a fingerprint, retina~~

9   ~~or iris image, or other unique physical representation or digital representation~~

10   ~~of~~ biometric data;

11   (vi) genetic information; and

12   (vii)(I) health records or records of a wellness program or similar

13   program of health promotion or disease prevention;

14   (II) a health care professional's medical diagnosis or treatment

15   of the consumer; or

16   (III) a health insurance policy number.

17   (B) "Personally identifiable information" does not mean publicly

18   available information that is lawfully made available to the general public from

19   federal, State, or local government records.

20   (14) "Processor" has the same meaning as in section 2415 of this title.

1   (11)(15) "Record" means any material on which written, drawn, spoken,

2   visual, or electromagnetic information is recorded or preserved, regardless of

3   physical form or characteristics.

4   (12)(16) "Redaction" means the rendering of data so that the data are

5   unreadable or are truncated so that no not more than the last four digits of the

6   identification number are accessible as part of the data.

7   (13)(17)(A) "Security breach" means unauthorized acquisition of

8   electronic data, or a reasonable belief of an unauthorized acquisition of

9   electronic data, that compromises the security, confidentiality, or integrity of a

10   consumer's personally identifiable information or login credentials maintained

11   by a data collector.

12   (B) "Security breach" does not include good faith but unauthorized

13   acquisition of personally identifiable information or login credentials by an

14   employee or agent of the data collector for a legitimate purpose of the data

15   collector, provided that the personally identifiable information or login

16   credentials are not used for a purpose unrelated to the data collector's business

17   or subject to further unauthorized disclosure.

18   (C) In determining whether personally identifiable information or

19   login credentials have been acquired or is reasonably believed to have been

20   acquired by a person without valid authorization, a data collector may consider

21   the following factors, among others:

1   (i) indications that the information is in the physical possession

2   and control of a person without valid authorization, such as a lost or stolen

3   computer or other device containing information;

4   (ii) indications that the information has been downloaded or

5   copied;

6   (iii) indications that the information was used by an unauthorized

7   person, such as fraudulent accounts opened or instances of identity theft

8   reported; or

9   (iv) that the information has been made public.

10   * * *

11   Subchapter 2. ~~Security Breach Notice Act~~ Data Security Breaches

12   * * *

13   § 2436. NOTICE OF DATA BROKER SECURITY BREACH

14   (a) Short title. This section shall be known as the Data Broker Security

15   Breach Notice Act.

16   (b) Notice of breach.

17   (1) Except as otherwise provided in subsection (c) of this section, any

18   data broker shall notify the consumer that there has been a data broker security

19   breach following discovery or notification to the data broker of the breach.

20   Notice of the security breach shall be made in the most expedient time possible

21   and without unreasonable delay, but not later than 45 days after the discovery

1   or notification, consistent with the legitimate needs of the law enforcement

2   agency, as provided in subdivisions (3) and (4) of this subsection, or with any

3   measures necessary to determine the scope of the security breach and restore

4   the reasonable integrity, security, and confidentiality of the data system.

5   (2) A data broker shall provide notice of a breach to the Attorney

6   General as follows:

7   (A)(i) The data broker shall notify the Attorney General of the date of

8   the security breach and the date of discovery of the breach and shall provide a

9   preliminary description of the breach within 14 business days, consistent with

10   the legitimate needs of the law enforcement agency, as provided in

11   subdivisions (3) and (4) of this subsection (b), after the data broker's discovery

12   of the security breach or when the data broker provides notice to consumers

13   pursuant to this section, whichever is sooner.

14   (ii) If the date of the breach is unknown at the time notice is sent

15   to the Attorney General, the data broker shall send the Attorney General the

16   date of the breach as soon as it is known.

17   (iii) Unless otherwise ordered by a court of this State for good

18   cause shown, a notice provided under this subdivision (2)(A) shall not be

19   disclosed to any person other than the authorized agent or representative of the

20   Attorney General, a State's Attorney, or another law enforcement officer

1   engaged in legitimate law enforcement activities without the consent of the

2   data broker.

3   (B)(i) When the data broker provides notice of the breach pursuant to

4   subdivision (1) of this subsection (b), the data broker shall notify the Attorney

5   General of the number of Vermont consumers affected, if known to the data

6   broker, and shall provide a copy of the notice provided to consumers under

7   subdivision (1) of this subsection (b).

8   (ii) The data broker may send to the Attorney General a second

9   copy of the consumer notice, from which is redacted the type of brokered

10   personal information that was subject to the breach, that the Attorney General

11   shall use for any public disclosure of the breach.

12   (3) The notice to a consumer required by this subsection shall be

13   delayed upon request of a law enforcement agency. A law enforcement agency

14   may request the delay if it believes that notification may impede a law

15   enforcement investigation or a national or Homeland Security investigation or

16   jeopardize public safety or national or Homeland Security interests. In the

17   event law enforcement makes the request for a delay in a manner other than in

18   writing, the data broker shall document the request contemporaneously in

19   writing and include the name of the law enforcement officer making the

20   request and the officer's law enforcement agency engaged in the investigation.

21   A law enforcement agency shall promptly notify the data broker in writing

1   when the law enforcement agency no longer believes that notification may

2   impede a law enforcement investigation or a national or Homeland Security

3   investigation, or jeopardize public safety or national or Homeland Security

4   interests. The data broker shall provide notice required by this section without

5   unreasonable delay upon receipt of a written communication, which includes

6   facsimile or electronic communication, from the law enforcement agency

7   withdrawing its request for delay.

8   (4) The notice to a consumer required in subdivision (1) of this

9   subsection shall be clear and conspicuous. A notice to a consumer of a

10   security breach involving brokered personal information shall include a

11   description of each of the following, if known to the data broker:

12   (A) the incident in general terms;

13   (B) the type of brokered personal information that was subject to the

14   security breach;

15   (C) the general acts of the data broker to protect the brokered

16   personal information from further security breach;

17   (D) a telephone number, toll-free if available, that the consumer may

18   call for further information and assistance;

19   (E) advice that directs the consumer to remain vigilant by reviewing

20   account statements and monitoring free credit reports; and

21   (F) the approximate date of the data broker security breach.

1	(5) A data broker may provide notice of a security breach involving

2	brokered personal information to a consumer by two or more of the following

3	methods:

4	(A) written notice mailed to the consumer's residence;

5	(B) electronic notice, for those consumers for whom the data broker

6	has a valid e-mail address, if:

7	(i) the data broker's primary method of communication with the

8	consumer is by electronic means, the electronic notice does not request or

9	contain a hypertext link to a request that the consumer provide personal

10	information, and the electronic notice conspicuously warns consumers not to

11	provide personal information in response to electronic communications

12	regarding security breaches; or

13	(ii) the notice is consistent with the provisions regarding electronic

14	records and signatures for notices in 15 U.S.C. § 7001;

15	(C) telephonic notice, provided that telephonic contact is made

16	directly with each affected consumer and not through a prerecorded message;

17	or

18	(D) notice by publication in a newspaper of statewide circulation in

19	the event the data broker cannot effectuate notice by any other means.

20	(c) Exception.

1   (1) Notice of a security breach pursuant to subsection (b) of this section

2   is not required if the data broker establishes that misuse of brokered personal

3   information is not reasonably possible and the data broker provides notice of

4   the determination that the misuse of the brokered personal information is not

5   reasonably possible pursuant to the requirements of this subsection. If the data

6   broker establishes that misuse of the brokered personal information is not

7   reasonably possible, the data broker shall provide notice of its determination

8   that misuse of the brokered personal information is not reasonably possible and

9   a detailed explanation for said determination to the Vermont Attorney General.

10   The data broker may designate its notice and detailed explanation to the

11   Vermont Attorney General as a trade secret if the notice and detailed

12   explanation meet the definition of trade secret contained in 1 V.S.A.

13   § 317(c)(9).

14   (2) If a data broker established that misuse of brokered personal

15   information was not reasonably possible under subdivision (1) of this

16   subsection and subsequently obtains facts indicating that misuse of the

17   brokered personal information has occurred or is occurring, the data broker

18   shall provide notice of the security breach pursuant to subsection (b) of this

19   section.

20   (d) Waiver. Any waiver of the provisions of this subchapter is contrary to

21   public policy and is void and unenforceable.

1   (e) Enforcement.

2   (1) With respect to a controller or processor other than a controller or

3   processor licensed or registered with the Department of Financial Regulation

4   under title 8 or this title, the Attorney General and State's Attorney shall have

5   sole and full authority to investigate potential violations of this chapter and to

6   enforce, prosecute, obtain, and impose remedies for a violation of this chapter

7   or any rules or regulations adopted pursuant to this chapter as the Attorney

8   General and State's Attorney have under chapter 63 of this title. The Attorney

9   General may refer the matter to the State's Attorney in an appropriate case.

10   The Superior Courts shall have jurisdiction over any enforcement matter

11   brought by the Attorney General or a State's Attorney under this subsection.

12   (2) With respect to a controller or processor that is licensed or registered

13   with the Department of Financial Regulation under title 8 or this title, the

14   Department of Financial Regulation shall have the full authority to investigate

15   potential violations of this chapter and to enforce, prosecute, obtain, and

16   impose remedies for a violation of this chapter or any rules or regulations

17   adopted pursuant to this chapter, as the Department has under title 8 or this title

18   or any other applicable law or regulation.

19   * * *

20   Subchapter 5. Data Brokers

21   § 2446. DATA BROKERS; ANNUAL REGISTRATION

1   (a) Annually, on or before January 31 following a year in which a person

2   meets the definition of data broker as provided in section 2430 of this title, a

3   data broker shall:

4   (1) register with the Secretary of State;

5   (2) pay a registration fee of $100.00; and

6   (3) provide the following information:

7   (A) the name and primary physical, e-mail, and ~~Internet~~ internet

8   addresses of the data broker;

9   (B) if the data broker permits a consumer to opt out of the data

10   broker's collection of brokered personal information, opt out of its databases,

11   or opt out of certain sales of data:

12   (i) the method for requesting an opt-out;

13   (ii) if the opt-out applies to only certain activities or sales, which

14   ones; and

15   (iii) whether the data broker permits a consumer to authorize a

16   third party to perform the opt-out on the consumer's behalf;

17   (C) a statement specifying the data collection, databases, or sales

18   activities from which a consumer may not opt out;

19   (D) a statement whether the data broker implements a purchaser

20   credentialing process;

1   (E) the number of data broker security breaches that the data broker

2   has experienced during the prior year, and if known, the total number of

3   consumers affected by the breaches;

4   (F) where the data broker has actual knowledge that it possesses the

5   brokered personal information of minors, a separate statement detailing the

6   data collection practices, databases, sales activities, and opt-out policies that

7   are applicable to the brokered personal information of minors; and

8   (G) any additional information or explanation the data broker

9   chooses to provide concerning its data collection practices.

10   (b) A data broker that fails to register pursuant to subsection (a) of this

11   section is liable to the State for:

12   (1) a civil penalty of $50.00 $125.00 for each day, not to exceed a total

13   of $10,000.00 for each year, it fails to register pursuant to this section;

14   (2) an amount equal to the fees due under this section during the period

15   it failed to register pursuant to this section; and

16   (3) other penalties imposed by law.

17   (c) A data broker that omits required information from its registration shall

18   file an amendment to include the omitted information within five business days

19   following notification of the omission and is liable to the State for a civil

20   penalty of $1,000.00 per day for each day thereafter.

1   (d) A data broker that files materially incorrect information in its

2   registration:

3   (1) is liable to the State for a civil penalty of $25,000.00; and

4   (2) if it fails to correct the false information within five business days

5   after discovery or notification of the incorrect information, an additional civil

6   penalty of $1,000.00 per day for each day thereafter that it fails to correct the

7   information.

8   (e) The Attorney General may maintain an action in the Civil Division of

9   the Superior Court to collect the penalties imposed in this section and to seek

10   appropriate injunctive relief.

11   * * *

12   § 2448. DATA BROKERS; CREDENTIALING

13   (a) Credentialing.

14   (1) A data broker shall maintain reasonable procedures designed to

15   ensure that the brokered personal information it discloses is used for a

16   legitimate and legal purpose.

17   (2) These procedures shall require that prospective users of the

18   information identify themselves, certify the purposes for which the information

19   is sought, and certify that the information shall be used for no other purpose.

1   (3) A data broker shall make a reasonable effort to verify the identity of

2   a new prospective user and the uses certified by the prospective user prior to

3   furnishing the user brokered personal information.

4   (4) A data broker shall not furnish brokered personal information to any

5   person if it has reasonable grounds for believing that the consumer report will

6   not be used for a legitimate and legal purpose.

7   (b) Exemption. Nothing in this section applies to:

8   (1) brokered personal information that is:

9   (A) regulated as a consumer report pursuant to the Fair Credit

10   Reporting Act, 15 U.S.C. § 1681–1681x, if the data broker is fully complying

11   with the Act; or

12   (B) regulated pursuant to the Driver's Privacy Protection Act of

13   1994, 18 U.S.C. § 2721–2725, if the data broker is fully complying with the

14   Act;

15   (2) a public service company subject to the rules and orders of the

16   Vermont Public Utility Commission regarding data sharing and service quality;

17   (3) a nonprofit organization that is established to detect and prevent

18   fraudulent acts in connection with insurance; or

19   (4) a nonprofit organization that is established to provide enrollment

20   data reporting services on behalf of postsecondary schools as that term is

21   defined in 16 V.S.A. § 176.

1   <mark>Sec. 4. EFFECTIVE DATE</mark>

2   (a) This section and Sec. 2 (AI and Data Privacy Advisory Council) shall

3   take effect on July 1, 2024.

4   (b) Sec. 1 (Vermont Data Privacy Act) and Sec. 3 (Protection of Personal

5   Information) shall take effect on July 1, 2025.

6

7

8

9

10

11

12

13   (Committee vote: _____)

14   _____

15   Senator _____

16   FOR THE COMMITTEE