

1 TO THE HONORABLE SENATE:

2 The Committee on Institutions to which was referred Senate Bill No. 71  
3 entitled “An act relating to consumer data privacy” respectfully reports that it  
4 has considered the same and recommends that the bill be amended by striking  
5 out all after the enacting clause and inserting in lieu thereof the following:

6 An act relating to consumer data privacy

7 It is hereby enacted by the General Assembly of the State of Vermont:

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” means terminating a pregnancy for any purpose other  
13 than producing a live birth.

14 (2)(A) “Affiliate” means a legal entity that shares common branding  
15 with another legal entity or controls, is controlled by, or is under common  
16 control with another legal entity.

17 (B) As used in subdivision (A) of this subdivision (2), “control” or  
18 “controlled” means:

19 (i) ownership of, or the power to vote, more than 50 percent of the  
20 outstanding shares of any class of voting security of a company;

1                    (ii) control in any manner over the election of a majority of the  
2                    directors or of individuals exercising similar functions; or

3                    (iii) the power to exercise controlling influence over the  
4                    management of a company.

5                    (3) “Authenticate” means to use reasonable means to determine that a  
6                    request to exercise any of the rights afforded under subdivisions 2418(a)(1)–  
7                    (4) of this title is being made by, or on behalf of, the consumer who is entitled  
8                    to exercise the consumer rights with respect to the personal data at issue.

9                    (4)(A) “Biometric data” means personal data generated by automatic  
10                    measurements of an individual’s unique biological patterns or characteristics  
11                    that are used to identify a specific individual.

12                    (B) “Biometric data” does not include:

13                    (i) a digital or physical photograph;

14                    (ii) an audio or video recording; or

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

18                    (5) “Business associate” has the same meaning as in HIPAA.

19                    (6) “Child” has the same meaning as in COPPA.

1           (7)(A) “Consent” means a clear affirmative act signifying a consumer’s  
2           freely given, specific, informed, and unambiguous agreement to allow the  
3           processing of personal data relating to the consumer.

4           (B) “Consent” may include a written statement, including by  
5           electronic means, or any other unambiguous affirmative action.

6           (C) “Consent” does not include:

7           (i) acceptance of a general or broad terms of use or similar  
8           document that contains descriptions of personal data processing along with  
9           other, unrelated information;

10           (ii) hovering over, muting, pausing, or closing a given piece of  
11           content; or

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

13           (8)(A) “Consumer” means an individual who is a resident of the State.

14           (B) “Consumer” does not include an individual acting in a  
15           commercial or employment context or as an employee, owner, director, officer,  
16           or contractor of a company, partnership, sole proprietorship, nonprofit, or  
17           government agency whose communications or transactions with the controller  
18           occur solely within the context of that individual’s role with the company,  
19           partnership, sole proprietorship, nonprofit, or government agency.

1           (9) “Consumer health data” means any personal data that a controller  
2           uses to identify a consumer’s physical or mental health condition or diagnosis,  
3           including gender-affirming health data and reproductive or sexual health data.

4           (10) “Consumer health data controller” means any controller that, alone  
5           or jointly with others, determines the purpose and means of processing  
6           consumer health data.

7           (11) “Controller” means a person who, alone or jointly with others,  
8           determines the purpose and means of processing personal data.

9           (12) “COPPA” means the Children’s Online Privacy Protection Act of  
10           1998, 15 U.S.C. § 6501–6506, and any regulations, rules, guidance, and  
11           exemptions adopted pursuant to the act, as the act and regulations, rules,  
12           guidance, and exemptions may be amended.

13           (13) “Covered entity” has the same meaning as in HIPAA.

14           (14) “Dark pattern” means a user interface designed or manipulated with  
15           the substantial effect of subverting or impairing user autonomy, decision-  
16           making, or choice and includes any practice the Federal Trade Commission  
17           refers to as a “dark pattern.”

18           (15) “Decisions that produce legal or similarly significant effects  
19           concerning the consumer” means decisions made by the controller that result in  
20           the provision or denial by the controller of financial or lending services,  
21           housing, insurance, education enrollment or opportunity, criminal justice,

1 employment opportunities, health care services, or access to essential goods or  
2 services.

3 (16) “De-identified data” means data that does not identify and cannot  
4 reasonably be used to infer information about, or otherwise be linked to, an  
5 identified or identifiable individual, or a device linked to the individual, if the  
6 controller that possesses the data:

7 (A) takes reasonable measures to ensure that the data cannot be  
8 associated with an individual;

9 (B) publicly commits to process the data only in a de-identified  
10 fashion and not attempt to re-identify the data; and

11 (C) contractually obligates any recipients of the data to satisfy the  
12 criteria set forth in subdivisions (A) and (B) of this subdivision (16).

13 (17) “Gender-affirming health care services” has the same meaning as in  
14 1 V.S.A. § 150.

15 (18) “Gender-affirming health data” means any personal data  
16 concerning a past, present, or future effort made by a consumer to seek, or a  
17 consumer’s receipt of, gender-affirming health care services.

18 (19) “Geofence” means any technology that uses global positioning  
19 coordinates, cell tower connectivity, cellular data, radio frequency  
20 identification, wireless fidelity technology data, or any other form of location  
21 detection, or any combination of such coordinates, connectivity, data,

1 identification, or other form of location detection, to establish a virtual  
2 boundary.

3 (20) “HIPAA” means the Health Insurance Portability and  
4 Accountability Act of 1996, Pub. L. No. 104-191, as may be amended.

5 (21) “Identified or identifiable individual” means an individual who can  
6 be readily identified, directly or indirectly.

7 (22) “Institution of higher education” means any individual who, or  
8 school, board, association, limited liability company or corporation that, is  
9 licensed or accredited to offer one or more programs of higher learning leading  
10 to one or more degrees.

11 (23) “Mental health facility” means any health care facility in which at  
12 least 70 percent of the health care services provided in the facility are mental  
13 health services.

14 (24) “Nonprofit organization” means any organization that is qualified  
15 for tax exempt status under I.R.C. § 501(c)(3), 501(c)(4), 501(c)(6), or  
16 501(c)(12), or any corresponding internal revenue code of the United States, as  
17 may be amended.

18 (25) “Person” means an individual, association, company, limited  
19 liability company, corporation, partnership, sole proprietorship, trust, or other  
20 legal entity.

1           (26)(A) “Personal data” means any information that is linked or  
2           reasonably linkable to an identified or identifiable individual.

3           (B) “Personal data” does not include de-identified data or publicly  
4           available information.

5           (27)(A) “Precise geolocation data” means information derived from  
6           technology, including global positioning system level latitude and longitude  
7           coordinates or other mechanisms, that directly identifies the specific location  
8           of an individual with precision and accuracy within a radius of 1,750 feet.

9           (B) “Precise geolocation data” does not include:

10           (i) the content of communications;

11           (ii) data generated by or connected to an advanced utility metering  
12           infrastructure system; or

13           (iii) data generated by equipment used by a utility company.

14           (28) “Process” or “processing” means any operation or set of operations  
15           performed, whether by manual or automated means, on personal data or on sets  
16           of personal data, such as the collection, use, storage, disclosure, analysis,  
17           deletion, or modification of personal data.

18           (29) “Processor” means a person who processes personal data on behalf  
19           of a controller.

20           (30) “Profiling” means any form of automated processing performed on  
21           personal data to evaluate, analyze, or predict personal aspects related to an

1 identified or identifiable individual’s economic situation, health, personal  
2 preferences, interests, reliability, behavior, location, or movements.

3 (31) “Protected health information” has the same meaning as in HIPAA.

4 (32) “Pseudonymous data” means personal data that cannot be attributed  
5 to a specific individual without the use of additional information, provided the  
6 additional information is kept separately and is subject to appropriate technical  
7 and organizational measures to ensure that the personal data is not attributed to  
8 an identified or identifiable individual.

9 (33) “Publicly available information” means information that:

10 (A) is lawfully made available through federal, state, or local  
11 government records or widely distributed media; or

12 (B) a controller has a reasonable basis to believe that the consumer  
13 has lawfully made available to the general public.

14 (34) “Reproductive or sexual health care” means any health care-related  
15 services or products rendered or provided concerning a consumer’s  
16 reproductive system or sexual well-being, including any such service or  
17 product rendered or provided concerning:

18 (A) an individual health condition, status, disease, diagnosis,  
19 diagnostic test or treatment;

20 (B) a social, psychological, behavioral, or medical intervention;

21 (C) a surgery or procedure, including an abortion;



1           (D) a use or purchase of a medication, including a medication used or  
2 purchased for the purposes of an abortion, a bodily function, vital sign, or  
3 symptom;

4           (E) a measurement of a bodily function, vital sign, or symptom; or

5           (F) an abortion, including medical or nonmedical services, products,  
6 diagnostics, counseling, or follow-up services for an abortion.

7           (35) “Reproductive or sexual health data” means any personal data  
8 concerning an effort made by a consumer to seek, or a consumer’s receipt of,  
9 reproductive or sexual health care.

10           (36) “Reproductive or sexual health facility” means any health care  
11 facility in which at least 70 percent of the health care-related services or  
12 products rendered or provided in the facility are reproductive or sexual health  
13 care.

14           (37)(A) “Sale of personal data” means the exchange of a consumer’s  
15 personal data by the controller to a third party for monetary or other valuable  
16 consideration.

17           (B) “Sale of personal data” does not include:

18           (i) the disclosure of personal data to a processor that processes the  
19 personal data on behalf of the controller;

20           (ii) the disclosure of personal data to a third party for purposes of  
21 providing a product or service requested by the consumer;

1                    (iii) the disclosure or transfer of personal data to an affiliate of the  
2                    controller;

3                    (iv) the disclosure of personal data where the consumer directs the  
4                    controller to disclose the personal data or intentionally uses the controller to  
5                    interact with a third party;

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

7                    (I) intentionally made available to the general public via a  
8                    channel of mass media; and

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

10                  (vi) the disclosure or transfer of personal data to a third party as an  
11                  asset that is part of a merger, acquisition, bankruptcy or other transaction, or a  
12                  proposed merger, acquisition, bankruptcy, or other transaction, in which the  
13                  third party assumes control of all or part of the controller’s assets.

14                  (38) “Sensitive data” means personal data that includes:

15                  (A) data revealing racial or ethnic origin, religious beliefs, mental or  
16                  physical health condition or diagnosis, sex life, sexual orientation, or  
17                  citizenship or immigration status;

18                  (B) consumer health data;

19                  (C) the processing of genetic or biometric data for the purpose of  
20                  uniquely identifying an individual;

21                  (D) personal data collected from a known child;

1           (E) data concerning an individual’s status as a victim of crime; and

2           (F) an individual’s precise geolocation data.

3           (39)(A) “Targeted advertising” means displaying advertisements to a  
4           consumer where the advertisement is selected based on personal data obtained  
5           or inferred from that consumer’s activities over time and across nonaffiliated  
6           websites or online applications to predict the consumer’s preferences or  
7           interests.

8           (B) “Targeted advertising” does not include:

9           (i) an advertisement based on activities within the controller’s own  
10          commonly branded website or online application;

11          (ii) an advertisement based on the context of a consumer’s current  
12          search query, visit to a website, or use of an online application;

13          (iii) an advertisement directed to a consumer in response to the  
14          consumer’s request for information or feedback; or

15          (iv) processing personal data solely to measure or report  
16          advertising frequency, performance, or reach.

17          (40) “Third party” means a person, public authority, agency, or body,  
18          other than the consumer, controller, or processor or an affiliate of the processor  
19          or the controller.

20          (41) “Trade secret” has the same meaning as in section 4601 of this title.

1     § 2416. APPLICABILITY

2           (a) Except as provided in subsection (b) of this section, this chapter applies  
3     to a person that conducts business in this State or a person that produces  
4     products or services that are targeted to residents of this State and that during  
5     the preceding calendar year:

6           (1) controlled or processed the personal data of not fewer than 100,000  
7     consumers, excluding personal data controlled or processed solely for the  
8     purpose of completing a payment transaction; or

9           (2) controlled or processed the personal data of not fewer than 25,000  
10    consumers and derived more than 25 percent of the person’s gross revenue  
11    from the sale of personal data.

12           (b) Section 2426 of this title and the provisions of this chapter concerning  
13    consumer health data and consumer health data controllers apply to a person  
14    that conducts business in this State or a person that produces products or  
15    services that are targeted to residents of this State.

16    § 2417. EXEMPTIONS

17           (a) Except as provided in subsection (c) of this section, this chapter shall  
18    not apply to any:

19           (1) body, authority, board, bureau, commission, district or agency of this  
20    State or of any political subdivision of this State;

1           (2) person who has entered into a contract with an entity described in  
2           subdivision (1) of this subsection to process consumer health data on behalf of  
3           the entity;

4           (3) nonprofit organization;

5           (4) institution of higher education;

6           (5) national securities association that is registered under 15 U.S.C. 78o-  
7           3 of the Securities Exchange Act of 1934, as may be amended;

8           (6) financial institution or data subject to Title V of the Gramm-Leach-  
9           Bliley Act, Pub. L. No. 106-102, and regulations adopted to implement that  
10          act;

11          (7) covered entity or business associate, as defined in 45 C.F.R.  
12          § 160.103;

13          (8) tribal nation government organization; or

14          (9) air carrier, as:

15                 (A) defined in 49 U.S.C. § 40102, as may be amended; and

16                 (B) regulated under the Federal Aviation Act of 1958, 49 U.S.C.  
17                 § 40101 et seq. and the Airline Deregulation Act of 1978, 49 U.S.C. § 41713,  
18                 as may be amended.

19          (b) The following information, data, and activities are exempt from this  
20          chapter:

21                 (1) protected health information under HIPAA;

1           (2) patient identifying information that is collected and processed in  
2           accordance with 42 C.F.R. Part 2 (confidentiality of substance use disorder  
3           patient records);

4           (3) identifiable private information:

5           (A) for purposes of the Federal Policy for the Protection of Human  
6           Subjects, codified as 45 C.F.R. Part 46 (HHS protection of human subjects)  
7           and in various other federal regulations; and

8           (B) that is otherwise information collected as part of human subjects  
9           research pursuant to the good clinical practice guidelines issued by the  
10           International Council for Harmonisation of Technical Requirements for  
11           Pharmaceuticals for Human Use;

12           (4) information that identifies a consumer in connection with the  
13           protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal  
14           data used or shared in research, as defined in 45 C.F.R. § 164.501, that is  
15           conducted in accordance with the standards set forth in this subdivision and in  
16           subdivision (3) of this subsection, or other research conducted in accordance  
17           with applicable law;

18           (5) information or documents created for the purposes of the Healthcare  
19           Quality Improvement Act of 1986, 42 U.S.C. §§ 11101–11152, and regulations  
20           adopted to implement that act;

1           (6) patient safety work product that is created for purposes of improving  
2           patient safety under 42 C.F.R. Part 3 (patient safety organizations and patient  
3           safety work product);

4           (7) information derived from any of the health care-related information  
5           listed in this subsection that is de-identified in accordance with the  
6           requirements for de-identification pursuant to HIPAA;

7           (8) information originating from and intermingled to be  
8           indistinguishable with, or information treated in the same manner as,  
9           information exempt under this subsection that is maintained by a covered  
10          entity or business associate, program, or qualified service organization, as  
11          specified in 42 U.S.C. § 290dd-2, as may be amended;

12          (9) information used for public health activities and purposes as  
13          authorized by HIPAA, community health activities, and population health  
14          activities;

15          (10) the collection, maintenance, disclosure, sale, communication, or use  
16          of any personal information bearing on a consumer’s credit worthiness, credit  
17          standing, credit capacity, character, general reputation, personal characteristics,  
18          or mode of living by a consumer reporting agency, furnisher, or user that  
19          provides information for use in a consumer report, and by a user of a consumer  
20          report, but only to the extent that such activity is regulated by and authorized

1 under the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., as may be  
2 amended;

3 (11) personal data collected, processed, sold, or disclosed under and in  
4 compliance with:

5 (A) the Driver’s Privacy Protection Act of 1994, 18 U.S.C. § 2721–  
6 2725; and

7 (B) the Farm Credit Act, Pub. L. No. 92-181, as may be amended;

8 (12) personal data regulated by the Family Educational Rights and  
9 Privacy Act, 20 U.S.C. § 1232g, as may be amended;

10 (13) data processed or maintained:

11 (A) in the course of an individual applying to, employed by, or acting  
12 as an agent or independent contractor of a controller, processor, consumer  
13 health data controller, or third party, to the extent that the data is collected and  
14 used within the context of that role;

15 (B) as the emergency contact information of a consumer pursuant to  
16 this chapter, used for emergency contact purposes, or

17 (C) that is necessary to retain to administer benefits for another  
18 individual relating to the individual who is the subject of the information  
19 pursuant to subdivision (1) of this subsection (b) and used for the purposes of  
20 administering such benefits; and



1           (14) personal data collected, processed, sold, or disclosed in relation to  
2           price, route, or service, as such terms are used in the Federal Aviation Act of  
3           1958, 49 U.S.C. § 40101 et seq., as may be amended, and the Airline  
4           Deregulation Act of 1978, 49 U.S.C. § 41713, as may be amended.

5           (c) Controllers, processors, and consumer health data controllers that  
6           comply with the verifiable parental consent requirements of COPPA shall be  
7           deemed compliant with any obligation to obtain parental consent pursuant to  
8           this chapter.

9           § 2418. CONSUMER RIGHTS; COMPLIANCE BY CONTROLLERS;

10           APPEALS

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

12           (1) confirm whether or not a controller is processing the consumer's  
13           personal data and access the personal data, unless the confirmation or access  
14           would require the controller to reveal a trade secret;

15           (2) correct inaccuracies in the consumer's personal data, taking into  
16           account the nature of the personal data and the purposes of the processing of  
17           the consumer's personal data;

18           (3) delete personal data provided by, or obtained about, the consumer;

19           (4) obtain a copy of the consumer's personal data processed by the  
20           controller, in a portable and, to the extent technically feasible, readily usable  
21           format that allows the consumer to transmit the data to another controller

1 without hindrance, where the processing is carried out by automated means,  
2 provided the controller shall not be required to reveal any trade secret; and

3 (5) opt out of the processing of the personal data for purposes of:

4 (A) targeted advertising;

5 (B) the sale of personal data, except as provided in subsection  
6 2420(b) of this title; or

7 (C) profiling in furtherance of solely automated decisions that  
8 produce legal or similarly significant effects concerning the consumer.

9 (b)(1) A consumer may exercise rights under this section by a secure and  
10 reliable means established by the controller and described to the consumer in  
11 the controller’s privacy notice.

12 (2) A consumer may designate an authorized agent in accordance with  
13 section 2419 of this title to exercise the rights of the consumer to opt out of the  
14 processing of the consumer’s personal data for purposes of subdivision (a)(5)  
15 of this section on behalf of the consumer.

16 (3) In the case of processing personal data of a known child, the parent  
17 or legal guardian may exercise the consumer rights on the child’s behalf.

18 (4) In the case of processing personal data concerning a consumer  
19 subject to a guardianship, conservatorship, or other protective arrangement, the  
20 guardian or the conservator of the consumer may exercise the rights on the  
21 consumer’s behalf.

1       (c) Except as otherwise provided in this chapter, a controller shall comply  
2       with a request by a consumer to exercise the consumer rights authorized  
3       pursuant to this chapter as follows:

4               (1)(A) A controller shall respond to the consumer without undue delay,  
5               but not later than 45 days after receipt of the request.

6               (B) The controller may extend the response period by 45 additional  
7               days when reasonably necessary, considering the complexity and number of  
8               the consumer’s requests, provided the controller informs the consumer of the  
9               extension within the initial 45-day response period and of the reason for the  
10              extension.

11              (2) If a controller declines to take action regarding the consumer’s  
12              request, the controller shall inform the consumer without undue delay, but not  
13              later than 45 days after receipt of the request, of the justification for declining  
14              to take action and instructions for how to appeal the decision.

15              (3)(A) Information provided in response to a consumer request shall be  
16              provided by a controller, free of charge, once per consumer during any 12-  
17              month period.

18              (B) If requests from a consumer are manifestly unfounded, excessive,  
19              or repetitive, the controller may charge the consumer a reasonable fee to cover  
20              the administrative costs of complying with the request or decline to act on the  
21              request.

1           (C) The controller bears the burden of demonstrating the manifestly  
2           unfounded, excessive, or repetitive nature of the request.

3           (4)(A) If a controller is unable to authenticate a request to exercise any  
4           of the rights afforded under subdivisions (a)(1)–(4) of this section using  
5           commercially reasonable efforts, the controller shall not be required to comply  
6           with a request to initiate an action pursuant to this section and shall provide  
7           notice to the consumer that the controller is unable to authenticate the request  
8           to exercise the right or rights until the consumer provides additional  
9           information reasonably necessary to authenticate the consumer and the  
10           consumer’s request to exercise the right or rights.

11           (B) A controller shall not be required to authenticate an opt-out  
12           request, but a controller may deny an opt-out request if the controller has a  
13           good faith, reasonable, and documented belief that the request is fraudulent.

14           (C) If a controller denies an opt-out request because the controller  
15           believes the request is fraudulent, the controller shall send a notice to the  
16           person who made the request disclosing that the controller believes the request  
17           is fraudulent, why the controller believes the request is fraudulent, and that the  
18           controller shall not comply with the request.

19           (5) A controller that has obtained personal data about a consumer from a  
20           source other than the consumer shall be deemed in compliance with a

1 consumer's request to delete the data pursuant to subdivision (a)(3) of this  
2 section by:

3 (A) retaining a record of the deletion request and the minimum data  
4 necessary for the purpose of ensuring the consumer's personal data remains  
5 deleted from the controller's records and not using the retained data for any  
6 other purpose pursuant to the provisions of this chapter; or

7 (B) opting the consumer out of the processing of the personal data for  
8 any purpose except for those exempted pursuant to the provisions of this  
9 chapter.

10 (d)(1) A controller shall establish a process for a consumer to appeal the  
11 controller's refusal to take action on a request within a reasonable period of  
12 time after the consumer's receipt of the decision.

13 (2) The appeal process shall be conspicuously available and similar to  
14 the process for submitting requests to initiate action pursuant to this section.

15 (3) Not later than 60 days after receipt of an appeal, a controller shall  
16 inform the consumer in writing of any action taken or not taken in response to  
17 the appeal, including a written explanation of the reasons for the decisions.

18 (4) If the appeal is denied, the controller shall also provide the consumer  
19 with an online mechanism, if available, or other method through which the  
20 consumer may contact the Attorney General to submit a complaint.

21 § 2419. AUTHORIZED AGENTS AND CONSUMER OPT-OUT

1        (a) A consumer may designate another person to serve as the consumer’s  
2        authorized agent, and act on the consumer’s behalf, to opt out of the processing  
3        of the consumer’s personal data for one or more of the purposes specified in  
4        subdivision 2418(a)(5) of this title.

5        (b) The consumer may designate an authorized agent by way of, among  
6        other things, a technology, including an internet link or a browser setting,  
7        browser extension, or global device setting, indicating the consumer’s intent to  
8        opt out of the processing.

9        (c) A controller shall comply with an opt-out request received from an  
10       authorized agent if the controller is able to verify, with commercially  
11       reasonable effort, the identity of the consumer and the authorized agent’s  
12       authority to act on the consumer’s behalf.

13       § 2420. CONTROLLERS’ DUTIES; SALE OF PERSONAL DATA TO  
14       THIRD PARTIES; NOTICE AND DISCLOSURE TO  
15       CONSUMERS; CONSUMER OPT-OUT

16       (a) A controller:

17       (1) shall limit the collection of personal data to what is adequate,  
18       relevant, and reasonably necessary in relation to the purposes for which the  
19       data is processed, as disclosed to the consumer;

20       (2) except as otherwise provided in this chapter, shall not process  
21       personal data for purposes that are neither reasonably necessary to, nor

1 compatible with, the disclosed purposes for which the personal data is  
2 processed, as disclosed to the consumer, unless the controller obtains the  
3 consumer’s consent;

4 (3) shall establish, implement, and maintain reasonable administrative,  
5 technical, and physical data security practices to protect the confidentiality,  
6 integrity, and accessibility of personal data appropriate to the volume and  
7 nature of the personal data at issue;

8 (4) shall not process sensitive data concerning a consumer without  
9 obtaining the consumer’s consent or, in the case of the processing of sensitive  
10 data concerning a known child, without processing the data in accordance with  
11 COPPA;

12 (5) shall not process personal data in violation of the laws of this State  
13 and federal laws that prohibit unlawful discrimination against consumers;

14 (6) shall provide an effective mechanism for a consumer to revoke the  
15 consumer’s consent under this section that is at least as easy as the mechanism  
16 by which the consumer provided the consumer’s consent and, upon revocation  
17 of the consent, cease to process the data as soon as practicable, but not later  
18 than 15 days after the receipt of the request;

19 (7) shall not process the personal data of a consumer for purposes of  
20 targeted advertising, or sell the consumer’s personal data without the  
21 consumer’s consent, under circumstances where a controller has actual

1 knowledge, and willfully disregards, that the consumer is at least 13 years of  
2 age but younger than 16 years of age; and

3 (8) shall not discriminate against a consumer for exercising any of the  
4 consumer rights contained in this chapter, including denying goods or services,  
5 charging different prices or rates for goods or services, or providing a different  
6 level of quality of goods or services to the consumer.

7 (b) Subsection (a) of this section shall not be construed to require a  
8 controller to provide a product or service that requires the personal data of a  
9 consumer that the controller does not collect or maintain, or prohibit a  
10 controller from offering a different price, rate, level, quality, or selection of  
11 goods or services to a consumer, including offering goods or services for no  
12 fee if the offering is in connection with a consumer’s voluntary participation in  
13 a bona fide loyalty, rewards, premium features, discounts, or club card  
14 program.

15 (c) A controller shall provide consumers with a reasonably accessible,  
16 clear, and meaningful privacy notice that includes:

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

18 (2) the purpose for processing personal data;

19 (3) how consumers may exercise their consumer rights, including how a  
20 consumer may appeal a controller’s decision with regard to the consumer’s  
21 request;



1           (4) the categories of personal data that the controller shares with third  
2 parties, if any;

3           (5) the categories of third parties, if any, with which the controller  
4 shares personal data; and

5           (6) an active email address or other online mechanism that the consumer  
6 may use to contact the controller.

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

11           (e)(1) A controller shall establish, and shall describe in a privacy notice,  
12 one or more secure and reliable means for consumers to submit a request to  
13 exercise their consumer rights pursuant to this chapter.

14           (2) The means shall take into account the ways in which consumers  
15 normally interact with the controller, the need for secure and reliable  
16 communication of the requests, and the ability of the controller to verify the  
17 identity of the consumer making the request.

18           (3) A controller shall not require a consumer to create a new account in  
19 order to exercise consumer rights but may require a consumer to use an  
20 existing account.

21           (4)(A) The means shall include:

1                    (i) providing a clear and conspicuous link on the controller’s  
2                    website to an web page that enables a consumer, or an agent of the consumer,  
3                    to opt out of the targeted advertising or sale of the consumer’s personal data;  
4                    and

5                    (ii) not later than January 1, 2026, allowing a consumer to opt out  
6                    of any processing of the consumer’s personal data for the purposes of targeted  
7                    advertising, or any sale of the personal data, through an opt-out preference  
8                    signal sent to the controller with the consumer’s consent indicating the  
9                    consumer’s intent to opt out of any the processing or sale, by a platform,  
10                   technology, or other mechanism that shall:

11                    (I) not unfairly disadvantage another controller;

12                    (II) not make use of a default setting, but rather require the  
13                    consumer to make an affirmative, freely given, and unambiguous choice to opt  
14                    out of any processing of the consumer’s personal data pursuant to this chapter;

15                    (III) be consumer-friendly and easy to use by the average  
16                    consumer;

17                    (IV) be as consistent as possible with any other similar  
18                    platform, technology, or mechanism required by any federal or State law or  
19                    regulation; and

20                    (V) enable the controller to accurately determine whether the  
21                    consumer is a resident of this State and whether the consumer has made a

1 legitimate request to opt out of any sale of the consumer’s personal data or  
2 targeted advertising.

3 (B) If a consumer’s decision to opt out of any processing of the  
4 consumer’s personal data for the purposes of targeted advertising, or any sale  
5 of the personal data, through an opt-out preference signal sent in accordance  
6 with the provisions of subdivision (A) of this subdivision (e)(4) conflicts with  
7 the consumer’s existing controller-specific privacy setting or voluntary  
8 participation in a controller’s bona fide loyalty, rewards, premium features,  
9 discounts, or club card program, the controller shall comply with the  
10 consumer’s opt-out preference signal but may notify the consumer of the  
11 conflict and provide to the consumer the choice to confirm the controller-  
12 specific privacy setting or participation in the program.

13 (5) If a controller responds to consumer opt-out requests received  
14 pursuant to subdivision (4)(A) of this subsection by informing the consumer of  
15 a charge for the use of any product or service, the controller shall present the  
16 terms of any financial incentive offered pursuant to subsection (b) of this  
17 section for the retention, use, sale, or sharing of the consumer’s personal data.

1     § 2421. PROCESSORS' DUTIES; CONTRACTS BETWEEN  
2                     CONTROLLERS AND PROCESSORS

3             (a) A processor shall adhere to the instructions of a controller and shall  
4     assist the controller in meeting the controller's obligations under this chapter,  
5     including:

6             (1) taking into account the nature of processing and the information  
7     available to the processor, by appropriate technical and organizational  
8     measures, to the extent reasonably practicable, to fulfill the controller's  
9     obligation to respond to consumer rights requests;

10            (2) taking into account the nature of processing and the information  
11    available to the processor, by assisting the controller in meeting the  
12    controller's obligations in relation to the security of processing the personal  
13    data and in relation to the notification of a data broker security breach or  
14    security breach, as defined in section 2430 of this title, of the system of the  
15    processor, in order to meet the controller's obligations; and

16            (3) providing necessary information to enable the controller to conduct  
17    and document data protection assessments.

18            (b)(1) A contract between a controller and a processor shall govern the  
19    processor's data processing procedures with respect to processing performed  
20    on behalf of the controller.

1           (2) The contract shall be binding and clearly set forth instructions for  
2           processing data, the nature and purpose of processing, the type of data subject  
3           to processing, the duration of processing, and the rights and obligations of both  
4           parties.

5           (3) The contract shall require that the processor:

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

8           (B) at the controller’s direction, delete or return all personal data to  
9           the controller as requested at the end of the provision of services, unless  
10          retention of the personal data is required by law;

11          (C) upon the reasonable request of the controller, make available to  
12          the controller all information in its possession necessary to demonstrate the  
13          processor’s compliance with the obligations in this chapter;

14          (D) after providing the controller an opportunity to object, engage  
15          any subcontractor pursuant to a written contract that requires the subcontractor  
16          to meet the obligations of the processor with respect to the personal data; and

17          (E) make available to the controller upon the reasonable request of  
18          the controller, all information in the processor’s possession necessary to  
19          demonstrate the processor’s compliance with this chapter.

20          (4) A processor shall provide a report of an assessment to the controller  
21          upon request.

1        (c) This section shall not be construed to relieve a controller or processor  
2        from the liabilities imposed on the controller or processor by virtue of the  
3        controller’s or processor’s role in the processing relationship, as described in  
4        this chapter.

5        (d)(1) Determining whether a person is acting as a controller or processor  
6        with respect to a specific processing of data is a fact-based determination that  
7        depends upon the context in which personal data is to be processed.

8        (2) A person who is not limited in the person’s processing of personal  
9        data pursuant to a controller’s instructions, or who fails to adhere to the  
10       instructions, is a controller and not a processor with respect to a specific  
11       processing of data.

12       (3) A processor that continues to adhere to a controller’s instructions  
13       with respect to a specific processing of personal data remains a processor.

14       (4) If a processor begins, alone or jointly with others, determining the  
15       purposes and means of the processing of personal data, the processor is a  
16       controller with respect to the processing and may be subject to an enforcement  
17       action under section 2425 of this title.

1     § 2422. CONTROLLERS' DATA PROTECTION ASSESSMENTS;

2                     DISCLOSURE TO ATTORNEY GENERAL

3             (a) A controller shall conduct and document a data protection assessment  
4             for each of the controller's processing activities that presents a heightened risk  
5             of harm to a consumer, which for the purposes of this section includes:

6                     (1) the processing of personal data for the purposes of targeted  
7             advertising;

8                     (2) the sale of personal data;

9                     (3) the processing of personal data for the purposes of profiling, where  
10            the profiling presents a reasonably foreseeable risk of:

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

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

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

17                     (D) other substantial injury to consumers; and

18                     (4) the processing of sensitive data.

19             (b)(1) Data protection assessments conducted pursuant to subsection (a) of  
20             this section shall identify and weigh the benefits that may flow, directly and  
21             indirectly, from the processing to the controller, the consumer, other

1 stakeholders, and the public against the potential risks to the rights of the  
2 consumer associated with the processing, as mitigated by safeguards that can  
3 be employed by the controller to reduce the risks.

4 (2) The controller shall factor into any data protection assessment the  
5 use of de-identified data and the reasonable expectations of consumers, as well  
6 as the context of the processing and the relationship between the controller and  
7 the consumer whose personal data will be processed.

8 (c)(1) The Attorney General may require that a controller disclose any data  
9 protection assessment that is relevant to an investigation conducted by the  
10 Attorney General, and the controller shall make the data protection assessment  
11 available to the Attorney General.

12 (2) The Attorney General may evaluate the data protection assessment  
13 for compliance with the responsibilities set forth in this chapter.

14 (3) Data protection assessments shall be confidential and shall be  
15 exempt from disclosure and copying under the Public Records Act.

16 (4) To the extent any information contained in a data protection  
17 assessment disclosed to the Attorney General includes information subject to  
18 attorney-client privilege or work product protection, the disclosure shall not  
19 constitute a waiver of the privilege or protection.

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



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

7       (f) Data protection assessment requirements shall apply to processing  
8       activities created or generated after July 1, 2025 and are not retroactive.

9       § 2423. DE-IDENTIFIED AND PSEUDONYMOUS DATA;

10       CONTROLLERS' DUTIES; EXCEPTIONS; APPLICABILITY OF

11       CONSUMERS' RIGHTS; DISCLOSURE AND OVERSIGHT

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

13       (1) take reasonable measures to ensure that the data cannot be associated  
14       with an individual;

15       (2) publicly commit to maintaining and using de-identified data without  
16       attempting to re-identify the data; and

17       (3) contractually obligate any recipients of the de-identified data to  
18       comply with the provisions of this chapter.

19       (b) This chapter shall not be construed to:

20       (1) require a controller or processor to re-identify de-identified data or  
21       pseudonymous data; or

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

4           (c) This chapter shall not be construed to require a controller or processor  
5           to comply with an authenticated consumer rights request if the controller:

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

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

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

15           (d) The rights afforded under subdivisions 2418(a)(1)–(4) of this title shall  
16           not apply to pseudonymous data in cases where the controller is able to  
17           demonstrate that any information necessary to identify the consumer is kept  
18           separately and is subject to effective technical and organizational controls that  
19           prevent the controller from accessing the information.

20           (e) A controller that discloses pseudonymous data or de-identified data  
21           shall exercise reasonable oversight to monitor compliance with any contractual

1 commitments to which the pseudonymous data or de-identified data is subject  
2 and shall take appropriate steps to address any breaches of those contractual  
3 commitments.

4 § 2424. CONSTRUCTION OF CONTROLLERS' AND PROCESSORS'

5 DUTIES

6 (a) This chapter shall not be construed to restrict a controller's, processor's,  
7 or consumer health data controller's ability to:

8 (1) comply with federal, state, or municipal laws, ordinances, or  
9 regulations;

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

13 (3) cooperate with law enforcement agencies concerning conduct or  
14 activity that the controller, processor, or consumer health data controller  
15 reasonably and in good faith believes may violate federal, state, or municipal  
16 laws, ordinances, or regulations;

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

18 (5) provide a product or service specifically requested by a consumer;

19 (6) perform under a contract to which a consumer is a party, including  
20 fulfilling the terms of a written warranty;

1           (7) take steps at the request of a consumer prior to entering into a  
2           contract;

3           (8) take immediate steps to protect an interest that is essential for the life  
4           or physical safety of the consumer or another individual, and where the  
5           processing cannot be manifestly based on another legal basis;

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

10           (10) engage in public or peer-reviewed scientific or statistical research  
11           in the public interest that adheres to all other applicable ethics and privacy laws  
12           and is approved, monitored, and governed by an institutional review board that  
13           determines, or similar independent oversight entities that determine:

14           (A) whether the deletion of the information is likely to provide  
15           substantial benefits that do not exclusively accrue to the controller;

16           (B) the expected benefits of the research outweigh the privacy risks;  
17           and

18           (C) whether the controller or consumer health data controller has  
19           implemented reasonable safeguards to mitigate privacy risks associated with  
20           research, including any risks associated with re-identification;

1           (11) assist another controller, processor, consumer health data  
2           controller, or third party with any of the obligations under this chapter; or

3           (12) process personal data for reasons of public interest in the area of  
4           public health, community health, or population health, but solely to the extent  
5           that the processing is:

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

8                   (B) under the responsibility of a professional subject to  
9                   confidentiality obligations under federal, state, or local law.

10           (b) The obligations imposed on controllers, processors, or consumer health  
11           data controllers under this chapter shall not restrict a controller’s, processor’s,  
12           or consumer health data controller’s ability to collect, use, or retain data for  
13           internal use to:

14                   (1) conduct internal research to develop, improve, or repair products,  
15                   services, or technology;

16                   (2) effectuate a product recall;

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

19                   (4) perform internal operations that are reasonably aligned with the  
20           expectations of the consumer or reasonably anticipated based on the  
21           consumer’s existing relationship with the controller or consumer health data

1 controller, or are otherwise compatible with processing data in furtherance of  
2 the provision of a product or service specifically requested by a consumer or  
3 the performance of a contract to which the consumer is a party.

4 (c)(1) The obligations imposed on controllers, processors, or consumer  
5 health data controllers under this chapter shall not apply where compliance by  
6 the controller, processor, or consumer health data controller with this chapter  
7 would violate an evidentiary privilege under the laws of this State.

8 (2) This chapter shall not be construed to prevent a controller, processor,  
9 or consumer health data controller from providing personal data concerning a  
10 consumer to a person covered by an evidentiary privilege under the laws of the  
11 State as part of a privileged communication.

12 (d)(1) A controller, processor, or consumer health data controller that  
13 discloses personal data to a processor or third-party controller pursuant to this  
14 chapter shall not be deemed to have violated this chapter if the processor or  
15 third-party controller that receives and processes the personal data violates this  
16 chapter, provided, at the time the disclosing controller, processor, or consumer  
17 health data controller disclosed the personal data, the disclosing controller,  
18 processor, or consumer health data controller did not have actual knowledge  
19 that the receiving processor or third-party controller would violate this chapter.

20 (2) A third-party controller or processor receiving personal data from a  
21 controller, processor, or consumer health data controller in compliance with

1 this chapter is not in violation of this chapter for the transgressions of the  
2 controller, processor, or consumer health data controller from which the third-  
3 party controller or processor receives the personal data.

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

5 (1) impose any obligation on a controller or processor that adversely  
6 affects the rights or freedoms of any person, including the rights of any person:

7 (A) to freedom of speech or freedom of the press guaranteed in the  
8 First Amendment to the United States Constitution; or

9 (B) under 12 V.S.A. § 1615;

10 (2) apply to any person’s processing of personal data in the course of the  
11 person’s purely personal or household activities; or

12 (3) require an independent school as defined in 16 V.S.A. § 11(a)(8) or a  
13 private institution of higher education, as defined in 20 U.S.C. § 1001 et seq.,  
14 to delete personal data or opt out of processing of personal data that would  
15 unreasonably interfere with the provision of education services by or the  
16 ordinary operation of the school or institution.

17 (f)(1) Personal data processed by a controller or consumer health data  
18 controller pursuant to this section may be processed to the extent that the  
19 processing is:

20 (A) reasonably necessary and proportionate to the purposes listed in  
21 this section; and

1           (B) adequate, relevant, and limited to what is necessary in relation to  
2           the specific purposes listed in this section.

3           (2)(A) Personal data collected, used, or retained pursuant to subsection  
4           (b) of this section shall, where applicable, take into account the nature and  
5           purpose or purposes of the collection, use, or retention.

6           (B) The data shall be subject to reasonable administrative, technical,  
7           and physical measures to protect the confidentiality, integrity, and accessibility  
8           of the personal data and to reduce reasonably foreseeable risks of harm to  
9           consumers relating to the collection, use, or retention of personal data.

10          (g) If a controller or consumer health data controller processes personal  
11          data pursuant to an exemption in this section, the controller or consumer health  
12          data controller bears the burden of demonstrating that the processing qualifies  
13          for the exemption and complies with the requirements in subsection (f) of this  
14          section.

15          (h) Processing personal data for the purposes expressly identified in this  
16          section shall not solely make a legal entity a controller or consumer health data  
17          controller with respect to the processing.

18          § 2425. ENFORCEMENT BY ATTORNEY GENERAL; NOTICE OF  
19          VIOLATION; CURE PERIOD; REPORT; PENALTY

20          (a) The Attorney General shall have exclusive authority to enforce  
21          violations of this chapter.



1        (b)(1) During the period beginning on July 1, 2025 and ending on  
2        December 31, 2026, the Attorney General shall, prior to initiating any action  
3        for a violation of any provision of this chapter, issue a notice of violation to the  
4        controller or consumer health data controller if the Attorney General  
5        determines that a cure is possible.

6            (2) If the controller or consumer health data controller fails to cure the  
7        violation within 60 days after receipt of the notice of violation, the Attorney  
8        General may bring an action pursuant to this section.

9            (3) Annually, on or before February 1, the Attorney General shall  
10       submit a report to the General Assembly disclosing:

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

13            (B) the nature of each violation;

14            (C) the number of violations that were cured during the available  
15       cure period; and

16            (D) any other matter the Attorney General deems relevant for the  
17       purposes of the report.

18        (c) Beginning on January 1, 2027, the Attorney General may, in  
19        determining whether to grant a controller or processor the opportunity to cure  
20        an alleged violation described in subsection (b) of this section, consider:

21            (1) the number of violations;

1           (2) the size and complexity of the controller or processor;

2           (3) the nature and extent of the controller’s or processor’s processing  
3 activities;

4           (4) the substantial likelihood of injury to the public;

5           (5) the safety of persons or property;

6           (6) whether the alleged violation was likely caused by human or  
7 technical error; and

8           (7) the sensitivity of the data.

9           (d) This chapter shall not be construed as providing the basis for, or be  
10 subject to, a private right of action for violations of this chapter or any other  
11 law.

12           (e) Subjection to the exception in subsection (f) of this section, a violation  
13 of the requirements of this chapter shall constitute an unfair and deceptive act  
14 in commerce in violation of section 2453 of this title and shall be enforced  
15 solely by the Attorney General, provided that a consumer private right of  
16 action under subsection 2461(b) of this title shall not apply to the violation.

17           (f) The Attorney General shall provide guidance to controllers and  
18 processors for compliance with the terms of the Vermont Data Privacy Act.  
19 Any processor or controller that, in the opinion of the Attorney General,  
20 materially complies with the guidance provided by the Attorney General shall  
21 not constitute an unfair and deceptive act in commerce.

1     § 2426. CONSUMER HEALTH DATA PRIVACY

2           (a) Except as provided in subsections (b) and (c) of this section and  
3     subsections 2417(b) and (c) of this title, no person shall:

4           (1) provide any employee or contractor with access to consumer health  
5     data unless the employee or contractor is subject to a contractual or statutory  
6     duty of confidentiality;

7           (2) provide any processor with access to consumer health data unless the  
8     person and processor comply with section 2421 of this title;

9           (3) use a geofence to establish a virtual boundary that is within 1,750  
10    feet of any health care facility, including any mental health facility or  
11    reproductive or sexual health facility, for the purpose of identifying, tracking,  
12    collecting data from, or sending any notification to a consumer regarding the  
13    consumer’s consumer health data; or

14          (4) sell, or offer to sell, consumer health data without first obtaining the  
15    consumer’s consent.

16          (b) Notwithstanding section 2416 of this title, subsection (a) of this section,  
17    and the provisions of sections 2415–2425 of this title, inclusive, concerning  
18    consumer health data and consumer health data controllers, apply to persons  
19    that conduct business in this state and persons that produce products or  
20    services that are targeted to residents of this state.

21          (c) Subsection (a) of this section shall not apply to any:

1           (1) body, authority, board, bureau, commission, district or agency of this  
2           State or of any political subdivision of this State;

3           (2) person who has entered into a contract with an entity described in  
4           subdivision (1) of this subsection to process consumer health data on behalf of  
5           the entity;

6           (3) institution of higher education;

7           (4) national securities association that is registered under 15 U.S.C. 78o-  
8           3 of the Securities Exchange Act of 1934, as may be amended;

9           (5) financial institution or data subject to Title V of the Gramm-Leach-  
10          Bliley Act, Pub. L. No. 106-102, and regulations adopted to implement that  
11          act;

12          (6) covered entity or business associate, as defined in 45 C.F.R.  
13          § 160.103;

14          (7) tribal nation government organization; or

15          (8) air carrier, as:

16                 (A) defined in 49 U.S.C. § 40102, as may be amended; and

17                 (B) regulated under the Federal Aviation Act of 1958, 49 U.S.C.

18                 § 40101 et seq. and the Airline Deregulation Act of 1978, 49 U.S.C. § 41713,

19                 as may be amended.

20          Sec. 2. EFFECTIVE DATE

21                 This act shall take effect on July 1, 2026.

1 (Committee vote: \_\_\_\_\_)

2

\_\_\_\_\_

3

Senator \_\_\_\_\_

4

FOR THE COMMITTEE