

1 TO THE HOUSE OF REPRESENTATIVES:

2 The Committee on Commerce and Economic Development to which was  
3 referred Senate Bill No. 71 entitled “An act relating to consumer data privacy  
4 and online surveillance” respectfully reports that it has considered the same  
5 and recommends that the House propose to the Senate that the bill be amended  
6 by 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. DATA PRIVACY

10 Subchapter 1. Vermont Data Privacy and Online Surveillance Act

11 § 2415a. SHORT TITLE AND DEFINITIONS

12 (a) Short title. This subchapter shall be known and may be cited as the  
13 “Vermont Data Privacy and Online Surveillance Act.”

14 (b) Definitions. As used in this subchapter:

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

18 (B) As used in subdivision (A) of this subdivision (1), “control”,  
19 “controls”, or “controlled” means:

20 (i) ownership of, or the power to vote, more than 50 percent of the  
21 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                   (2) “Authenticate” means to use reasonable means to determine that a  
6 request to exercise any of the rights afforded under subdivisions 2415d(a)(1)–  
7 (4) of this subchapter is being made by, or on behalf of, the consumer who is  
8 entitled to exercise the consumer rights with respect to the personal data at  
9 issue.

10                   (3)(A) “Biometric data” means data generated from the technological  
11 processing of an individual’s unique biological, physical, or physiological  
12 characteristics that allow or confirm the unique identification of the consumer,  
13 including:

14                   (i) iris or retina scans;

15                   (ii) fingerprints;

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

17                   (iv) vein patterns;

18                   (v) voice prints or vocal biomarkers; and

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

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

21                   (i) a digital or physical photograph;

1                   (ii) an audio or video recording; or

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

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

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

7                   (6) “Collect” means buying, renting, gathering, obtaining, receiving, or  
8 accessing any personal data by any means. This includes receiving data from  
9 the consumer, either actively or passively, or by observing the consumer’s  
10 behavior.

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

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

16                  (C) “Consent” does not include:

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

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

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

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

3                    (B) “Consumer” does not include an individual acting in a  
4                    commercial or employment context or as an employee, owner, director, officer,  
5                    or contractor of a company, partnership, sole proprietorship, nonprofit  
6                    organization, or government agency whose communications or transactions  
7                    with the controller occur solely within the context of that individual’s role with  
8                    the company, partnership, sole proprietorship, nonprofit organization, or  
9                    government agency.

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

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

16                  (11) “Consumer reporting agency” has the same meaning as in the Fair  
17                  Credit Reporting Act, 15 U.S.C. § 1681a(f).

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

20                  (13) “COPPA” means the Children’s Online Privacy Protection Act of  
21                  1998, 15 U.S.C. § 6501–6506, and any regulations, rules, guidance, and

1 exemptions adopted pursuant to the act, as the act and regulations, rules,  
2 guidance, and exemptions may be amended.

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

4 (15) “Credit union” has the same meaning as in 8 V.S.A. § 30101.

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

9 (17) “Decision that produces any legal or similarly significant effect”  
10 means any decision made by the controller, or on behalf of the controller, that  
11 results in the provision or denial by the controller of any financial or lending  
12 service, any housing, any insurance, any education enrollment or opportunity,  
13 any criminal justice, any employment opportunity, or any health care service.

14 (18) “Deidentified data” means data that does not identify and cannot  
15 reasonably be used to infer information about, or otherwise be linked to, an  
16 identified or identifiable individual, or a device linked to the individual, if the  
17 controller that possesses the data:

18 (A)(i) takes reasonable measures to ensure that the data cannot be  
19 used to reidentify an identified or identifiable individual or be associated with  
20 an individual or device that identifies or is linked or reasonably linkable to an  
21 individual or household; and

1                   (ii) for purposes of this subdivision (A), “reasonable measures”  
2 includes the deidentification requirements set forth under 45 C.F.R § 164.514  
3 (other requirements relating to uses and disclosures of protected health  
4 information);

5                   (B) publicly commits to process the data only in a deidentified  
6 fashion and not attempt to reidentify the data; and

7                   (C) contractually obligates any recipients of the data to comply with  
8 all provisions of this subchapter.

9                   (19) “Derived data” means data that is created by the derivation of  
10 information, data, assumptions, correlations, inferences, predictions, or  
11 conclusions from facts, evidence, or another source of information or data  
12 about a consumer’s device.

13                   (20) “Financial institution” as used in subdivision 2415c(a)(13) of this  
14 title has the same meaning as in 15 U.S.C. § 6809.

15                   (21) “Gender-affirming health care services” has the same meaning as in  
16 1 V.S.A. § 150.

17                   (22) “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.

20                   (23) “Genetic data” means any data, regardless of its format, that results  
21 from the analysis of a biological sample of an individual, or from another

1 source enabling equivalent information to be obtained, and concerns genetic  
2 material, including deoxyribonucleic acids (DNA), ribonucleic acids (RNA),  
3 genes, chromosomes, alleles, genomes, alterations or modifications to DNA or  
4 RNA, single nucleotide polymorphisms (SNPs), epigenetic markers,  
5 uninterpreted data that results from analysis of the biological sample or other  
6 source, and any information extrapolated, derived, or inferred therefrom.

7 (24) “Geofence” means any technology that uses global positioning  
8 coordinates, cell tower connectivity, cellular data, radio frequency  
9 identification, wireless fidelity technology data, or any other form of location  
10 detection, or any combination of such coordinates, connectivity, data,  
11 identification, or other form of location detection, to establish a virtual  
12 boundary.

13 (25) “Health care facility” has the same meaning as in 18 V.S.A. § 9432.

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

16 (27) “Hybrid entity” has the same meaning as in HIPAA.

17 (28) “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, precise geolocation data, or  
20 an online identifier.

1           (29) “Institution of higher education” means any individual who, or  
2           school, board, association, limited liability company or corporation that, is  
3           licensed or accredited to offer one or more programs of higher learning leading  
4           to one or more degrees.

5           (30) “Mental health facility” means any health care facility in which at  
6           least 70 percent of the health care services provided in the facility are mental  
7           health services.

8           (31) “Minor” means any consumer who is younger than 18 years of age.

9           (32) “Neural data” means any information that is generated by  
10          measuring the activity of an individual’s central nervous system.

11          (33) “Nonprofit organization” means any organization that is qualified  
12          for tax exempt status under I.R.C. § 501(c)(3), 501(c)(4), 501(c)(6), or  
13          501(c)(12), or any corresponding internal revenue code of the United States, as  
14          may be amended.

15          (34) “Nonpublic personal information” has the same meaning as in  
16          15 U.S.C. § 6809.

17          (35) “Patient-identifying information” has the same meaning as in  
18          42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

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

1           (37)(A) “Personal data” means any information, including derived data  
2           and unique identifiers, that is linked or reasonably linkable, alone or in  
3           combination with other information, to an identified or identifiable individual  
4           or to a device that identifies, is linked to, or is reasonably linkable to one or  
5           more identified or identifiable individuals in a household.

6           (B) “Personal data” does not include deidentified data or publicly  
7           available information.

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

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

13           (i) the content of communications;

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

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

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

1           (40) “Processor” means a person who collects or processes personal data  
2           on behalf of:

3                   (A) a controller; or

4                   (B) another processor.

5           (41) “Profiling” means any form of automated processing performed on  
6           personal data to evaluate, analyze, or predict personal aspects, including an  
7           individual’s economic situation, health, personal preferences, interests,  
8           reliability, behavior, location, movements, or identifying characteristics.

9           (42) “Protected health information” has the same meaning as in HIPAA.

10           (43) “Pseudonymous data” means personal data that cannot be attributed  
11           to a specific individual without the use of additional information, provided the  
12           additional information is kept separately and is subject to appropriate technical  
13           and organizational measures to ensure that the personal data are not attributed  
14           to an identified or identifiable individual.

15           (44)(A) “Publicly available information” means information that:

16                   (i) is made available through federal, state, or local government  
17           records or to the general public from widely distributed media; or

18                   (ii) a controller has a reasonable basis to believe that the consumer  
19           has lawfully made available to the general public.

20           (B) “Publicly available information” does not include:

1                   (i) biometric data collected by a business about a consumer  
2                   without the consumer’s knowledge;

3                   (ii) information that is collated and combined to create a consumer  
4                   profile that is made available to a user of a publicly available website either in  
5                   exchange for payment or free of charge;

6                   (iii) information that is made available for sale;

7                   (iv) an inference that is generated from the information described  
8                   in subdivision (ii) or (iii) of this subdivision (44)(B);

9                   (v) any obscene visual depiction, as defined in 18 U.S.C. § 1460;

10                  (vi) personal data that is created through the combination of  
11                  personal data with publicly available information;

12                  (vii) genetic data, unless otherwise made publicly available by the  
13                  consumer to whom the information pertains;

14                  (viii) information provided by a consumer on a website or online  
15                  service made available to all members of the public, for free or for a fee, where  
16                  the consumer has maintained a reasonable expectation of privacy in the  
17                  information, such as by restricting the information to a specific audience; or

18                  (ix) intimate images, authentic or computer generated, known to  
19                  be nonconsensual.

20                  (45) “Reproductive or sexual health care” has the same meaning as  
21                  “reproductive health care services” in 1 V.S.A. § 150(c).

1           (46) “Reproductive or sexual health data” means any personal data  
2           concerning an effort made by a consumer to seek, or a consumer’s receipt of,  
3           reproductive or sexual health care.

4           (47) “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           (48)(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                   (49) “Sensitive data” means personal data that includes:

9                   (A) data revealing:

10                   (i) racial or ethnic origin, religious beliefs, sex life, sexual  
11 orientation, status as nonbinary or transgender, or citizenship or immigration  
12 status; or

13                   (ii) a mental or physical health condition, diagnosis, disability, or  
14 treatment;

15                   (B) consumer health data;

16                   (C) genetic or biometric data or information derived therefrom;

17                   (D) personal data collected from an individual the controller has  
18 actual knowledge, or willfully disregards, is a child;

19                   (E) precise geolocation data;

20                   (F) neural data;

1           (G) a consumer’s financial account number, financial account login  
2           information, or credit card or debit card number that, in combination with any  
3           required access or security code, password, or credential, would allow access  
4           to a consumer’s financial account; or

5           (H) government-issued identification number, including, but not  
6           limited to, Social Security number, passport number, State identification card  
7           number, or driver’s license number, that applicable law does not require to be  
8           publicly displayed.

9           (50)(A) “Targeted advertising” means displaying advertisements to a  
10          consumer where the advertisement is selected based on personal data obtained  
11          or inferred from that consumer’s activities over time and across nonaffiliated  
12          websites or online applications to predict the consumer’s preferences or  
13          interests.

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

15               (i) an advertisement based on activities within the controller’s own  
16               website or online application;

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

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

1            (iv) processing of personal data solely to measure or report  
2            advertising frequency, performance, or reach.

3            (51) “Third party” means a person, public authority, agency, or body,  
4            other than the consumer, controller, or processor or an affiliate of the processor  
5            or the controller.

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

7            § 2415b. APPLICABILITY

8            (a) Thresholds. Except as provided in subsection (b) of this section, this  
9            subchapter applies to a person that conducts business in this State or a person  
10           that produces products or services that are targeted to residents of this State  
11           and that during the preceding calendar year:

12           (1) controlled or processed the personal data of not fewer than 35,000  
13           consumers, excluding personal data controlled or processed solely for the  
14           purpose of completing a payment transaction;

15           (2) controlled or processed the sensitive data of not fewer than X  
16           consumers, excluding personal data controlled or processed solely for the  
17           purposes of completing a payment transaction; or

18           (3) offers a consumer’s personal data for sale in trade or commerce.

19           (b) Health data applicability. Section 2415k of this subchapter and the  
20           provisions of this subchapter concerning consumer health data and consumer  
21           health data controllers apply to a person that conducts business in this State or

1 a person that produces products or services that are targeted to residents of this  
2 State.

3 (c) Controlling law. In the event of a conflict between the provisions of  
4 this subchapter and any other law, including the Vermont Age-Appropriate  
5 Design Code Act, the provisions of the law that afford the greatest protection  
6 for the right of privacy for consumers shall control.

7 § 2415c. EXEMPTIONS

8 (a) This subchapter does not apply to:

9 (1) in the ordinary course of its operation, a federal, state, tribal, or local  
10 government entity or an instrumentality of the State;

11 (2)(A) a covered entity that is not a hybrid entity;

12 (B) any health care component of a hybrid entity; or

13 (C) a business associate;

14 (3) patient-identifying information, for purposes of 42 U.S.C. § 290DD–  
15 2;

16 (4)(A) information to the extent it is used for public health, community  
17 health, or population health activities and purposes, as authorized by HIPAA,  
18 when provided by or to a covered entity or when provided by or to a business  
19 associate in accordance with the business associate agreement with a covered  
20 entity;

1           (B) information that is a health care record, as that term is defined in  
2           18 V.S.A. § 9419, if the information is held by an entity that is a covered entity  
3           or business associate under HIPAA because it collects, uses, or discloses  
4           protected health information;

5           (C) information that is deidentified in accordance with the  
6           requirements for deidentification set forth in 45 C.F.R. § 164.514 and that is  
7           derived from individually identifiable health information as described in  
8           HIPAA; and

9           (D) personal information consistent with the human subject  
10          protection requirements of the U.S. Food and Drug Administration;

11          (5) information used only for public health activities and purposes  
12          described in 45 C.F.R. § 164.512 (disclosure of protected health information  
13          without authorization);

14          (6) information that identifies a consumer in connection with:

15               (A) activities that are subject to the Federal Policy for the Protection  
16               of Human Subjects, codified as 45 C.F.R. Part 46 (HHS protection of human  
17               subjects) and in various other federal regulations;

18               (B) activities that are subject to the protections provided in 21 C.F.R.  
19               Parts 50 (FDA clinical investigations protection of human subjects) and  
20               56 (FDA clinical investigations institutional review boards); or

1           (C) research conducted in accordance with the requirements set forth  
2           in subdivisions (A) and (B) of this subdivision (a)(6) or otherwise in  
3           accordance with applicable law;

4           (7) patient-identifying information that is collected and processed in  
5           accordance with 42 C.F.R. Part 2 (confidentiality of substance use disorder  
6           patient records);

7           (8) patient safety work product that is created and used for purposes of  
8           patient safety improvement in accordance with 42 C.F.R. § 3, established in  
9           accordance with 42 U.S.C. §§ 299b–21 through 299b–26;

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

13           (10) information processed or maintained solely in connection with, and  
14           for the purpose of, enabling notice of an emergency to persons that an  
15           individual specifies;

16           (11) any activity that involves collecting, maintaining, disclosing,  
17           selling, communicating, or using information for the purpose of evaluating a  
18           consumer’s creditworthiness, credit standing, credit capacity, character,  
19           general reputation, personal characteristics, or mode of living if done strictly in  
20           accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C.  
21           §§ 1681–1681x, as may be amended, by:

1           (A) a consumer reporting agency;

2           (B) a person who furnishes information to a consumer reporting  
3           agency under 15 U.S.C. § 1681s-2 (responsibilities of furnishers of  
4           information to consumer reporting agencies); or

5           (C) a person who uses a consumer report as provided in 15 U.S.C.  
6           § 1681b(a)(3) (permissible purposes of consumer reports);

7           (12) information collected, processed, sold, or disclosed under and in  
8           accordance with the following laws and regulations:

9           (A) the Driver’s Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–  
10          2725;

11          (B) data that is subject to the Family Educational Rights and Privacy  
12          Act, 20 U.S.C. § 1232g, and regulations adopted to implement that act;

13          (C) data that is subject to the Airline Deregulation Act, Pub. L. No.  
14          95-504, only to the extent that an air carrier collects information related to  
15          prices, routes, or services, and only to the extent that the provisions of the  
16          Airline Deregulation Act preempt this subchapter;

17          (D) data that is subject to the Farm Credit Act, Pub. L. No. 92-181, as  
18          may be amended; and

19          (E) data that is subject to federal policy under 21 U.S.C. § 830  
20          (regulation of listed chemicals and certain machines);

1           (13) nonpublic personal information that is processed by a financial  
2           institution subject to the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and  
3           regulations adopted to implement that act;

4           (14) a state- or federally chartered bank or credit union, or an affiliate or  
5           subsidiary that is principally engaged in financial activities, as described in  
6           12 U.S.C. § 1843(k);

7           (15) an agent, broker-dealer, investment adviser, or investment adviser  
8           representative, as those terms are defined in section 5102 of this title, who is  
9           regulated by the Department of Financial Regulation or the Securities and  
10          Exchange Commission;

11          (16) a person regulated pursuant to 8 V.S.A. part 3 (chapters 101–165)  
12          other than a person who, alone or in combination with another person,  
13          establishes and maintains a self-insurance program and who does not otherwise  
14          engage in the business of entering into policies of insurance;

15          (17) health care providers and health care facilities, as those terms are  
16          defined in 18 V.S.A. § 9402, provided such providers and facilities maintain  
17          all protected health information in accordance with the requirements of  
18          18 V.S.A. § 1881 and HIPAA regardless of whether such providers or facilities  
19          are covered entities under 45 C.F.R. § 160.103;

20          (18) protected health information under HIPAA;

1           (19) a third-party administrator, as that term is defined in the Third Party  
2           Administrator Rule adopted pursuant to 18 V.S.A. § 9417, provided that the  
3           third-party administrator is subject to and in compliance with the Department  
4           of Financial Regulation’s Regulation IH-2001-01 (Privacy of Consumer  
5           Financial and Health Information).;

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) a nonprofit organization that is established to detect and prevent  
11           fraudulent acts in connection with insurance;

12           (22) information that is processed for purposes of compliance,  
13           enrollment or degree verification, or research services by a nonprofit  
14           organization that is established to provide enrollment data reporting services  
15           on behalf of postsecondary schools as that term is defined in 16 V.S.A. § 176;

16           (23) noncommercial activity of:

17           (A) a publisher, editor, reporter, or other person who is connected  
18           with or employed by a newspaper, magazine, periodical, newsletter, pamphlet,  
19           report, or other publication in general circulation;

20           (B) a radio or television station that holds a license issued by the  
21           Federal Communications Commission;

1           (C) a nonprofit organization that provides programming to radio or  
2 television networks; or

3           (D) a press association or wire service; or

4           (24) data processed or maintained:

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

9           (B) as the emergency contact information of a consumer pursuant to  
10 this subchapter, used for emergency contact purposes; or

11           (C) that is necessary to retain to administer benefits for another  
12 individual relating to the individual who is the subject of the information  
13 pursuant to subdivision (18) of this subsection (a) and used for the purposes of  
14 administering such benefits.

15           (b) Controllers, processors, and consumer health data controllers that  
16 comply with the verifiable parental consent requirements of COPPA shall be  
17 deemed compliant with any obligation to obtain parental consent pursuant to  
18 this subchapter.

19           § 2415d. CONSUMER PERSONAL DATA RIGHTS

20           (a) Consumer rights. A consumer shall have the right to:

1           (1) confirm whether or not a controller is processing the consumer’s  
2           personal data and access such personal data, including any inferences about the  
3           consumer derived from such personal data and whether a controller or  
4           processor is processing a consumer’s personal data for the purposes of  
5           profiling to make a decision that produces any legal or similarly significant  
6           effect concerning a consumer, unless such confirmation or access would  
7           require the controller to reveal a trade secret or the controller is prohibited  
8           from disclosing such personal data under subsection (e) of this section;

9           (2) correct inaccuracies in the consumer’s personal data, taking into  
10           account the nature of the personal data and the purposes of the processing of  
11           the consumer’s personal data;

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

13           (4) obtain a copy of the consumer’s personal data processed by the  
14           controller, in a portable and, to the extent technically feasible, readily usable  
15           format that allows the consumer to transmit the data to another controller  
16           without hindrance, where the processing is carried out by automated means,  
17           provided the controller shall not be required to reveal any trade secret;

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

19           (A) targeted advertising;

20           (B) the sale of personal data, except as provided in subsection  
21           2415e(b) of this subchapter; or

1           (C) profiling in furtherance of any automated decision that produces  
2           any legal or similarly significant effect concerning the consumer;

3           (6) if the consumer’s personal data were processed for the purposes of  
4           profiling in furtherance of any automated decision that produced any legal or  
5           similarly significant effect concerning the consumer, and if feasible:

6           (A) question the result of such profiling;

7           (B) be informed of the reason that such profiling resulted in such  
8           decision;

9           (C) review the consumer’s personal data that were processed for the  
10           purposes of such profiling; and

11           (D) if the profiling decision concerned housing, taking into account  
12           the nature of the personal data and the purposes for which such personal data  
13           were processed, be allowed to correct any incorrect personal data that were  
14           processed for the purposes of such profiling and have the profiling decision  
15           reevaluated based on the corrected personal data; and

16           (7) obtain from the controller a list of the third parties to which such  
17           controller has sold the consumer’s personal data or, if such controller does not  
18           maintain a list of the third parties to which such controller has sold the  
19           consumer’s personal data, a list of all third parties to which such controller has  
20           sold personal data, provided the controller shall not be required to reveal any  
21           trade secret.

1        (b) Exercising consumer rights.

2            (1) A consumer may exercise rights under this section by a secure and  
3 reliable means established by the controller and described to the consumer in  
4 the controller’s privacy notice pursuant to subsection 2415e(c) of this  
5 subchapter.

6            (2)(A) A consumer may designate another person to serve as the  
7 consumer’s authorized agent, and act on the consumer’s behalf, to opt out of  
8 the processing of the consumer’s personal data for the purposes specified in  
9 subdivision (a)(5) of this section.

10           (B) The consumer may designate an authorized agent by way of,  
11 among other things, a technology, including an internet link or a browser  
12 setting, browser extension, or global device setting, indicating the consumer’s  
13 intent to opt out of the processing.

14           (C) A controller shall comply with an opt-out request received from  
15 an authorized agent if the controller is able to verify, with commercially  
16 reasonable effort, the identity of the consumer and the authorized agent’s  
17 authority to act on the consumer’s behalf.

18           (3) In the case of processing personal data of a consumer who:

19            (A) a controller has actual knowledge, or willfully disregards, is a  
20 child, the parent or legal guardian may exercise the consumer rights on the  
21 child’s behalf; and

1           (B) is subject to a guardianship, conservatorship, or other protective  
2           arrangement, the guardian or the conservator of the consumer may exercise the  
3           rights on the consumer’s behalf.

4           (c) Controller compliance. Except as otherwise provided in this  
5           subchapter, a controller shall comply with a request by a consumer to exercise  
6           the consumer rights authorized pursuant to this subchapter as follows:

7           (1) Timeline to respond. A controller:

8           (A) shall respond to the consumer without undue delay, but not later  
9           than 45 days after receipt of the request; and

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

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

20           (3) Cost of information.

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

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

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

10           (4) Authentication of request.

11           (A) If a controller is unable to authenticate a request to exercise any  
12           of the rights afforded under subdivisions (a)(1)–(4) of this section using  
13           commercially reasonable efforts, the controller shall not be required to comply  
14           with a request to initiate an action pursuant to this section and shall provide  
15           notice to the consumer that the controller is unable to authenticate the request  
16           to exercise the right or rights until the consumer provides additional  
17           information reasonably necessary to authenticate the consumer and the  
18           consumer’s request to exercise the right or rights.

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

1           (C) If a controller denies an opt-out request because the controller  
2           believes the request is fraudulent, the controller shall send a notice to the  
3           person who made the request disclosing that the controller believes the request  
4           is fraudulent, why the controller believes the request is fraudulent, and that the  
5           controller shall not comply with the request.

6           (5) Third-party data. A controller that has obtained personal data about  
7           a consumer from a source other than the consumer shall be deemed in  
8           compliance with a consumer’s request to delete the consumer’s data pursuant  
9           to subdivision (a)(3) of this section by:

10           (A) retaining a record of the deletion request and the minimum data  
11           necessary for the purpose of ensuring the consumer’s personal data remains  
12           deleted from the controller’s records and not using the retained data for any  
13           other purpose pursuant to the provisions of this subchapter; or

14           (B) opting the consumer out of the processing of the personal data for  
15           any purpose except for those exempted pursuant to the provisions of this  
16           subchapter.

17           (d) Appeals.

18           (1) A controller shall establish a process for a consumer to appeal the  
19           controller’s refusal to take action on a request pursuant to this section within a  
20           reasonable period of time after the consumer’s receipt of the decision.

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

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

6           (4) If the controller denies the appeal, the controller shall also provide  
7           the consumer with an online mechanism, if available, or other method through  
8           which the consumer may contact the Attorney General to submit a complaint.

9           (e) Disclosure of certain information. A controller shall not disclose the  
10          following personal data in response to a request to exercise the consumer's  
11          rights pursuant to subdivision (a)(1) of this section and shall instead inform the  
12          consumer or the person exercising such right on behalf of the consumer, with  
13          sufficient particularity, that the controller has collected the consumer's:

14           (1) Social Security number;

15           (2) driver's license number, State identification card number, or other  
16          government-issued identification number;

17           (3) financial account number;

18           (4) health insurance identification number or medical identification  
19          number;

20           (5) account password;

21           (6) security question or answer thereto; or

1           (7) biometric data.

2           § 2415e. DUTIES OF CONTROLLERS

3           (a) Data collection and processing. A controller shall:

4                   (1) limit the collection of personal data to what is reasonably necessary  
5                   and proportionate in relation to the purposes for which such data are processed,  
6                   as disclosed to the consumer, and unless the controller obtains the consumer’s  
7                   consent, not process the consumer’s personal data for any material new  
8                   purpose that is neither reasonably necessary to, nor compatible with, the  
9                   purposes that were disclosed to the consumer;

10                   (2) establish, implement, and maintain reasonable administrative,  
11                   technical, and physical data security practices to protect the confidentiality,  
12                   integrity, and accessibility of personal data appropriate to the volume and  
13                   nature of the personal data at issue;

14                   (3) not process sensitive data concerning a consumer:

15                           (A) unless such processing is reasonably necessary in relation to the  
16                           purposes for which such sensitive data are processed and without obtaining the  
17                           consumer’s consent; or

18                           (B) without processing the sensitive data in accordance with COPPA  
19                           if the controller has actual knowledge, or willfully disregards, that the  
20                           consumer is a child, and subject to further restrictions in subdivision (9) of this  
21                           subsection (a);

1           (4) not process personal data in violation of any:

2                   (A) law of this State that prohibits unlawful discrimination against  
3           consumers and any evidence, or lack of evidence, concerning proactive  
4           antibias testing or any similar proactive effort to avoid processing data in  
5           violation of any such law, including any evidence or lack of evidence  
6           concerning the quality, efficacy, recency, and scope of any testing or effort, the  
7           results of which shall be relevant to any claim available for a violation of such  
8           law and any defense available thereto; or

9                   (B) federal law that prohibits unlawful discrimination against  
10           consumers;

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

16           (6) not sell the sensitive data of a consumer without the consumer’s  
17           consent;

18           (7) subject to subdivision (9) of this subsection, where a controller has  
19           actual knowledge, and willfully disregards, that a consumer is at least 13 years  
20           of age but younger than 18 years of age;

1           (A) not process the personal data of the consumer for purposes of  
2 targeted advertising; and

3           (B) not sell the consumer’s personal data;

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

8           (9) if the controller is a covered business and the consumer is a covered  
9 minor as both terms are defined in section 2449a of this title, comply with the  
10 requirements set forth in chapter 62, subchapter 6 of this title (Vermont Age-  
11 Appropriate Design Code Act).

12           (b) Limitations. Subsection (a) of this section shall not be construed to:

13           (1) require a controller to provide a product or service that requires the  
14 personal data of a consumer that the controller does not collect or maintain; or

15           (2) prohibit a controller from offering a different price, rate, level,  
16 quality, or selection of goods or services to a consumer, including offering  
17 goods or services for no fee if the offering is in connection with a consumer’s  
18 voluntary participation in a bona fide loyalty, rewards, premium features,  
19 discounts, or club card program.

20           (c) Privacy notice.

- 1           (1) A controller shall provide consumers with a reasonably accessible,  
2           clear, and meaningful privacy notice that includes:
- 3                   (A) the categories of personal data processed by the controller;  
4                   (B) the purpose for processing personal data;  
5                   (C) a description of the means, established pursuant to subsection (d)  
6           of this section, for consumers to submit requests to exercise their consumer  
7           rights pursuant to this subchapter, including a description of how consumers  
8           may:
- 9                   (i) exercise a consumer’s rights under subsection 2415d(a) of this  
10           subchapter; and
- 11                   (ii) appeal a controller’s decisions with regard to requests to  
12           exercise such rights;
- 13                   (D) the categories of personal data that the controller sells to third  
14           parties, if any;
- 15                   (E) the categories of third parties, if any, to which the controller sells  
16           personal data;
- 17                   (F) a clear and conspicuous disclosure of any:
- 18                   (i) processing of personal data for purposes of targeted  
19           advertising; or
- 20                   (ii) sale of personal data to a third party for purposes of targeted  
21           advertising;

1           (G) an active email address or other online mechanism that the  
2           consumer may use to contact the controller;

3           (H) a statement disclosing whether the controller collects, uses, or  
4           sells personal data for the purpose of training large language models; and

5           (I) the most recent month and year during which the controller  
6           updated the privacy notice.

7           (2) A controller shall make the privacy notice required under  
8           subdivision (1) of this subsection publicly available:

9           (A) through a conspicuous hyperlink that includes the word  
10          “privacy”:

11          (i) on the home page of the controller’s website, if the controller  
12          maintains a website;

13          (ii) on the application store page or download page of a mobile  
14          device, if the controller maintains an application for use on a mobile device;  
15          and

16          (iii) on the application’s settings menu or in a similarly  
17          conspicuous and accessible location, if the controller maintains an application  
18          for use on a mobile device or other device used to connect to the internet;

19          (B) through a medium in which the controller regularly interacts with  
20          consumers, including mail, if the controller does not maintain a website;

1           (C) in each language in which the controller:

2                   (i) provides any product or service that is subject to the privacy  
3 notice; or

4                   (ii) carries out any activity that is related to any product or service  
5 described in subdivision (i) of this subdivision (C); and

6           (D) in a manner that is reasonably accessible to, and usable by,  
7 individuals with disabilities.

8           (3) Whenever a controller makes any retroactive material change to the  
9 controller’s privacy notice or practices, the controller shall:

10                   (A) notify the consumers affected by such material change with  
11 respect to any personal data to be collected after the effective date of such  
12 material change;

13                   (B) provide a reasonable opportunity for the consumers described in  
14 subdivision (A) of this subdivision (3) to withdraw consent to any further and  
15 materially different collection, processing, or transfer of previously collected  
16 personal data following such material change; and

17                   (C) take all reasonable electronic measures to provide the notice set  
18 forth in this subdivision (3) to the affected consumers, taking into account the  
19 technology available to the controller and the nature of the controller’s  
20 relationship with such affected consumers.

1           (4) Nothing in this subsection shall be construed to require a controller  
2           to provide a privacy notice that is specific to this State if the controller  
3           provides a generally applicable privacy notice that satisfies the requirements  
4           established in this subsection.

5           (d) Providing consumers access to exercise rights.

6           (1) A controller shall:

7           (A) establish and describe in a privacy notice, one or more secure and  
8           reliable means for consumers to submit a request to exercise their consumer  
9           rights pursuant to this subchapter; and

10           (B) not require a consumer to create a new account in order to  
11           exercise consumer rights but may require a consumer to use an existing  
12           account.

13           (2) The means pursuant to subdivision (1) of this subsection shall:

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

18           (B) provide a clear and conspicuous link on the controller's website  
19           to a web page that enables a consumer, or an agent of the consumer, to opt out  
20           of the processing of the consumer's personal data for purposes of targeted  
21           advertising or any sale of the consumer's personal data; and

1           (C) allow a consumer to opt out of any processing of the consumer’s  
2           personal data for the purposes of targeted advertising, or any sale of the  
3           personal data, through an opt-out preference signal sent to the controller with  
4           the consumer’s consent indicating the consumer’s intent to opt out of any of  
5           the processing or sale, by a platform, technology, or other mechanism that  
6           shall:

7                   (i) not unfairly disadvantage another controller;

8                   (ii) not make use of a default setting, but rather require the  
9           consumer to make an affirmative, freely given, and unambiguous choice to opt  
10           out of any processing of the consumer’s personal data pursuant to this  
11           subchapter;

12                   (iii) be consumer friendly and easy to use by the average  
13           consumer;

14                   (iv) be as consistent as possible with any other similar platform,  
15           technology, or mechanism required by any federal or State law or regulation;

16           and

17                   (v) enable the controller to accurately determine whether the  
18           consumer is a resident of this State and whether the consumer has made a  
19           legitimate request to opt out of any sale of the consumer’s personal data or  
20           targeted advertising.

1           (3) If a consumer’s decision to opt out of any processing of the  
2           consumer’s personal data for the purposes of targeted advertising, or any sale  
3           of the personal data, through an opt-out preference signal sent in accordance  
4           with the provisions of subdivision (2)(C) of this subsection conflicts with the  
5           consumer’s existing controller-specific privacy setting or voluntary  
6           participation in a controller’s bona fide loyalty, rewards, premium features,  
7           discounts, or club card program, the controller shall comply with the  
8           consumer’s opt-out preference signal but may notify the consumer of the  
9           conflict and provide to the consumer the choice to confirm the controller-  
10           specific privacy setting or participation in the program.

11           (4) If a controller responds to a consumer opt-out request received  
12           pursuant to subdivision (2)(C) of this subsection by informing the consumer of  
13           a charge for the use of any product or service, the controller shall present the  
14           terms of any financial incentive offered pursuant to subdivision (b)(2) of this  
15           section for the retention, use, sale, or sharing of the consumer’s personal data.

16           § 2415f. PROCESSORS’ DUTIES; CONTRACTS BETWEEN  
17           CONTROLLERS AND PROCESSORS

18           (a) Generally. A processor shall adhere to the instructions of a controller  
19           and shall assist the controller in meeting the controller’s obligations under this  
20           subchapter, including:

1           (1) taking into account the nature of processing and to the extent  
2           possible, to fulfill the controller’s obligation to respond to consumer rights  
3           requests pursuant to subsection 2415d(a) of this subchapter;

4           (2) taking into account the nature of processing and the information  
5           available to the processor, by assisting the controller in meeting the  
6           controller’s obligations in relation to the security of processing the personal  
7           data and in relation to the notification of a data broker security breach or  
8           security breach, as defined in section 2430 of this title, of the system of the  
9           processor, in order to meet the controller’s obligations; and

10           (3) providing necessary information to enable the controller to conduct  
11           and document data protection and impact assessments.

12           (b) Contractual terms.

13           (1) A contract between a controller and a processor shall govern the  
14           processor’s data processing procedures with respect to processing performed  
15           on behalf of the controller.

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

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

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

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

7                   (C) upon the reasonable request of the controller, make available to  
8                   the controller all information in its possession necessary to demonstrate the  
9                   processor’s compliance with the obligations in this subchapter;

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

13                  (E) make available to the controller upon the reasonable request of  
14                  the controller all information in the processor’s possession necessary to  
15                  demonstrate the processor’s compliance with this subchapter.

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

18                  (c) Liabilities. This section shall not be construed to relieve a controller or  
19                  processor from the liabilities imposed on the controller or processor by virtue  
20                  of the controller’s or processor’s role in the processing relationship, as  
21                  described in this subchapter.

1           (d) Processors performing as controllers.

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

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

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

11                   (4) If a processor begins, alone or jointly with others, determining the  
12           purposes and means of the processing of personal data, the processor is a  
13           controller with respect to the processing and may be subject to an enforcement  
14           action under section 2415j of this subchapter.

15           § 2415g. DATA PROTECTION AND IMPACT ASSESSMENTS;

16                   DISCLOSURE TO ATTORNEY GENERAL

17                   (a) Generally. A controller shall conduct and document a data protection  
18           assessment for each of the controller’s processing activities that presents a  
19           heightened risk of harm to a consumer, which for the purposes of this section  
20           includes:

- 1           (1) the processing of personal data for the purposes of targeted  
2           advertising;
- 3           (2) the sale of personal data;
- 4           (3) the processing of personal data for the purposes of profiling, where  
5           the profiling presents a reasonably foreseeable risk of:
- 6                 (A) unfair or deceptive treatment of, or unlawful disparate impact on,  
7                 a consumer;
- 8                 (B) financial, physical, or reputational injury to a consumer;
- 9                 (C) a physical or other intrusion upon the solitude or seclusion, or the  
10                private affairs or concerns, of a consumer, where the intrusion would be  
11                offensive to a reasonable person; or
- 12                (D) other substantial injury to a consumer; and
- 13           (4) the processing of sensitive data.
- 14           (b) Requirements.
- 15                (1) Data protection assessments conducted pursuant to subsection (a) of  
16                this section shall identify and weigh the benefits that may flow, directly and  
17                indirectly, from the processing to the controller, the consumer, other  
18                stakeholders, and the public against the potential risks to the rights of the  
19                consumer associated with the processing, as mitigated by safeguards that can  
20                be employed by the controller to reduce the risks.

1           (2) The controller shall factor into each data protection assessment the  
2           use of deidentified data and the reasonable expectations of consumers, as well  
3           as the context of the processing and the relationship between the controller and  
4           the consumer whose personal data will be processed.

5           (c) Impact assessments for profiling. Each controller that engages in any  
6           profiling for the purposes of making a decision that produces any legal or  
7           similarly significant effect concerning a consumer shall conduct an impact  
8           assessment for the profiling. The impact assessment shall include, to the  
9           extent reasonably known by or available to the controller, as applicable:

10           (1) a statement by the controller disclosing the purpose, intended use  
11           cases, and deployment context of, and benefits afforded by, the profiling;

12           (2) an analysis of whether the profiling poses any known or reasonably  
13           foreseeable heightened risk of harm to a consumer, and, if so:

14           (A) the nature of such heightened risk of harm to a consumer; and

15           (B) the steps that have been taken to mitigate such heightened risk of  
16           harm to a consumer;

17           (3) a description of:

18           (A) the main categories of personal data processed as inputs for the  
19           purposes of such profiling; and

20           (B) the outputs such profiling produces;

1           (4) an overview of the main categories of personal data the controller  
2           used to customize the profiling, if the controller used data to customize the  
3           profiling;

4           (5) any metrics used to evaluate the performance and known limitations  
5           of the profiling;

6           (6) a description of any transparency measures taken concerning the  
7           profiling, including any measures taken to disclose to consumers that the  
8           controller is engaged in profiling while the controller is engaged in the  
9           profiling; and

10           (7) a description of the postdeployment monitoring and user safeguards  
11           provided concerning such profiling, including the oversight, use, and learning  
12           processes established by the controller to address issues arising from such  
13           profiling.

14           (d) Disclosure to Attorney General.

15           (1) The Attorney General may require that a controller disclose any data  
16           protection or impact assessment that is relevant to an investigation conducted  
17           by the Attorney General, and the controller shall make the data protection or  
18           impact assessment available to the Attorney General.

19           (2) The Attorney General may evaluate the data protection or impact  
20           assessment for compliance with the responsibilities set forth in this subchapter.

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

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

7           (e) Assessment efficiency and applicability.

8           (1) A single data protection or impact assessment may address a  
9           comparable set of processing operations that include similar activities.

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

16           (3) Data protection and impact assessment requirements shall apply to  
17           processing activities created or generated after January 1, 2028, and are not  
18           retroactive.

19           § 2415h. DEIDENTIFIED DATA

20           (a) Requirements. A controller in possession of deidentified data shall:

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

3           (2) publicly commit to maintaining and using deidentified data without  
4           attempting to reidentify the data; and

5           (3) contractually obligate any recipients of the deidentified data to  
6           comply with the provisions of this subchapter.

7           (b) Limitations. This subchapter shall not be construed to:

8           (1) require a controller or processor to reidentify deidentified data or  
9           pseudonymous data;

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

13           (3) require a controller or processor to comply with an authenticated  
14           consumer rights request if the controller:

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

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

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

4           (c) Pseudonymous data. The rights afforded under subdivisions  
5           2415d(a)(1)–(4) of this subchapter shall not apply to pseudonymous data in  
6           cases where the controller is able to demonstrate that any information  
7           necessary to identify the consumer is kept separately and is subject to effective  
8           technical and organizational controls that prevent the controller from accessing  
9           the information.

10          (d) Oversight when disclosing. A controller that discloses pseudonymous  
11          data or deidentified data shall exercise reasonable oversight to monitor  
12          compliance with any contractual commitments to which the pseudonymous  
13          data or deidentified data is subject and shall take appropriate steps to address  
14          any breaches of those contractual commitments.

15          § 2415i. CONSTRUCTION OF DUTIES

16          (a) Generally. This subchapter shall not be construed to restrict a  
17          controller’s, processor’s, or consumer health data controller’s ability to:

18                  (1) comply with federal, state, or municipal laws, ordinances, or  
19          regulations, except as prohibited by 1 V.S.A. § 150;

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

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

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

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

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

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

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

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

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

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

7                   (B) the expected benefits of the research outweigh the privacy risks;  
8           and

9                   (C) whether the controller or consumer health data controller has  
10           implemented reasonable safeguards to mitigate privacy risks associated with  
11           research, including any risks associated with reidentification;

12           (11) assist another controller, processor, consumer health data  
13           controller, or third party with any of the obligations under this subchapter; or

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

17                   (A) subject to suitable and specific measures to safeguard the rights  
18                   of the consumer whose personal data are being processed; and

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

1        (b) Internal use of data. The obligations imposed on controllers,  
2        processors, or consumer health data controllers under this subchapter shall not  
3        restrict a controller’s, processor’s, or consumer health data controller’s ability  
4        to collect, use, or retain data for internal use to:

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

7            (2) effectuate a product recall;

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

10          (4) process personal data for the purposes of profiling in furtherance of  
11          any automated decision that may produce any legal or similarly significant  
12          effect concerning a consumer, provided the personal data are:

13            (A) processed only to the extent necessary to detect or correct any  
14            bias that may result from processing the data for such purposes, the bias cannot  
15            effectively be detected or corrected without processing the data, and the data  
16            are deleted once the processing has been completed;

17            (B) processed subject to appropriate safeguards to protect the rights  
18            of consumers secured by the Constitution or laws of this State or of the United  
19            States;

1           (C) subject to technical restrictions concerning the reuse of the data  
2           and industry-standard security and privacy measures, including  
3           pseudonymization;

4           (D) subject to measures to ensure that the data are secure, protected,  
5           and subject to suitable safeguards, including strict controls concerning, and  
6           documentation of, access to the data, to avoid misuse and ensure that only  
7           authorized persons may access the data while preserving the confidentiality of  
8           the data; and

9           (E) not transmitted, transferred, or otherwise accessed by any third  
10          party;

11          (5) perform internal operations that are reasonably aligned with the  
12          expectations of the consumer or reasonably anticipated based on the  
13          consumer’s existing relationship with the controller or consumer health data  
14          controller, or are otherwise compatible with processing data in furtherance of  
15          the provision of a product or service specifically requested by a consumer or  
16          the performance of a contract to which the consumer is a party; or

17          (6) perform internal operations in accordance with the internal  
18          operations exception established in COPPA if the controller, processor, or  
19          consumer health data controller is processing data in accordance with the  
20          exception.

21          (c) Evidentiary privilege.

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

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

9           (3) Nothing in this subchapter modifies 2020 Acts and Resolves No.  
10           166, Sec. 14 or authorizes the use of facial recognition technology by law  
11           enforcement.

12           (d) Third parties.

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

1           (2) A third-party controller or processor receiving personal data from a  
2           controller, processor, or consumer health data controller in compliance with  
3           this subchapter is not in violation of this subchapter for the transgressions of  
4           the controller, processor, or consumer health data controller from which the  
5           third-party controller or processor receives the personal data.

6           (e) Clarifications. This subchapter shall not be construed to:

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

9           (A) to freedom of speech or freedom of the press guaranteed in the  
10          First Amendment to the U.S. Constitution; or

11          (B) under 12 V.S.A. § 1615;

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

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

19          (f) Personal data processing.

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

4                   (A) reasonably necessary and proportionate to the purposes listed in  
5                   this section; and

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

8           (2)(A) The collection, use, or retention of personal data pursuant to  
9           subsection (b) of this section shall, where applicable, take into account the  
10           nature and purpose or purposes of the collection, use, or retention.

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

15           (3) If a controller or consumer health data controller processes personal  
16           data pursuant to an exemption in this section, the controller or consumer health  
17           data controller bears the burden of demonstrating that the processing qualifies  
18           for the exemption and complies with the requirements of this subsection.

19           (4) Processing personal data for the purposes expressly identified in this  
20           section shall not solely make a legal entity a controller or consumer health data  
21           controller with respect to the processing.

1     § 2415j. ATTORNEY GENERAL ENFORCEMENT; REPORTING

2           (a) Consumer Protection Act. A violation of this subchapter shall be  
3     deemed a violation of the Vermont Consumer Protection Act, pursuant to  
4     chapter 63 of this title. The Attorney General has the same authority to enforce  
5     this subchapter as provided under 9 V.S.A. chapter 63, subchapter 1. This  
6     subchapter shall not be construed as providing the basis for, or be subject to, a  
7     private right of action for violations of this subchapter or any other law.

8           (b) Reporting. Annually, on or before December 1, the Attorney General  
9     shall submit a report to the General Assembly disclosing:

10           (1) the number of notices of violation pursuant to this subchapter that  
11     the Attorney General has issued;

12           (2) the nature of each violation;

13           (3) the number of violations that resulted in an enforcement action being  
14     taken;

15           (4) the number of enforcement actions that proceeded to trial; and

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

18           (c) Guidance. The Attorney General shall provide, and update as  
19     necessary, guidance to controllers and processors for compliance with the  
20     terms of the Vermont Data Privacy and Online Surveillance Act.

