

1 ~~S.71~~ 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 ~~It is hereby enacted by the General Assembly of the State of Vermont:~~

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

10 CHAPTER 61A. ~~VERMONT~~ DATA PRIVACY ~~ACT~~

11 Subchapter 1. Vermont Data Privacy and Online Surveillance Act

12 § 2415a. ~~SHORT TITLE AND DEFINITIONS~~

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

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

16 ~~(1) “Abortion” means terminating a pregnancy for any purpose other~~  
17 ~~than producing a live birth.~~

18 ~~(2)(A) “Affiliate” means a legal entity that shares common branding~~  
19 ~~with another legal entity or controls, is controlled by, or is under common~~  
20 ~~control with another legal entity.~~

1 (B) As used in subdivision (A) of this subdivision (~~21~~), “control” or  
2 “controlled” means:

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

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

7 (iii) the power to exercise controlling influence over the  
8 management of a company.

9 (~~32~~) “Authenticate” means to use reasonable means to determine that a  
10 request to exercise any of the rights afforded under subdivisions 24185d(a)(1)–  
11 (45) of this ~~title~~subchapter is being made by, or on behalf of, the consumer  
12 who is entitled to exercise the consumer rights with respect to the personal data  
13 at issue.

14 (~~43~~)(A) “Biometric data” means ~~personal~~ data generated ~~by automatic~~  
15 measurements from the technological processing of an individual’s unique  
16 biological, ~~patterns or physical, or physiological~~ characteristics that ~~are used to~~  
17 identify a specific individual, allow or confirm the unique identification of the  
18 consumer, including:

19 (i) iris or retina scans;

20 (ii) fingerprints;

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

1                   (iv) vein patterns;

2                   (v) voice prints or vocal biomarkers; and

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

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

5                   (i) a digital or physical photograph;

6                   (ii) an audio or video recording; or

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

8                   an audio or video recording, unless such data is generated to identify a specific  
9                   individual.

10                  (54) “Business associate” has the same meaning as in HIPAA.

11                  (65) “Child” has the same meaning as in COPPA.

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

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

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

21                  (C) “Consent” does not include:

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

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

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

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

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

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

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

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

3           (12)(A) “Contextual advertising” or “contextual advertisement” means  
4 displaying or presenting an advertisement that does not vary based on the  
5 identity of the individual recipient and is based solely on:

6                   (i) the immediate content of a web page or online service within  
7 which the advertisement appears; or

8                   (ii) a specific request of the consumer for information or feedback.

9           (B) A controller may use the following types of information to  
10 display a contextual advertisement:

11                   (i) technical specifications as are necessary for the ad to be  
12 delivered and displayed properly on a given device;

13                   (ii) a consumer’s immediate presence in a geographic area with a  
14 radius not smaller than 10 miles, or an area reasonably estimated to include  
15 online activity from at least 5,000 users, but not including precise geolocation  
16 data; and

17                   (iii) the consumer’s language preferences, as inferred from  
18 context, browser settings, or user settings.

19           (C) A controller using information pursuant to subdivision (B) of this  
20 subdivision (12) to display a contextual advertisement shall not use that  
21 information to make inferences about a consumer, profile a consumer, or for

1 any other purpose, and the controller shall not prohibit a consumer from using  
2 technical means to obfuscate or change a consumer’s physical location to  
3 specify a language preference.

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

6 (1214) “COPPA” means the Children’s Online Privacy Protection Act  
7 of 1998, 15 U.S.C. § 6501–6506, and any regulations, rules, guidance, and  
8 exemptions adopted pursuant to the act, as the act and regulations, rules,  
9 guidance, and exemptions may be amended.

10 (1315) “Covered entity” has the same meaning as in HIPAA.

11 (16) “Credit union” has the same meaning as in 8 V.S.A. § 30101.14

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

16 (1518) “Decisions that produce legal or similarly significant effects  
17 concerning the consumer” means any decisions made by the controller, or on  
18 behalf of the controller, that results in the provision or denial by the controller  
19 of any financial or lending services, any housing, any insurance, any education  
20 enrollment or opportunity, any criminal justice, any employment

1 ~~opportunities, y, or any health care services, or access to essential goods or~~  
2 ~~services.~~

3 (1619) “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)(i) takes reasonable measures to ensure that the data cannot be  
8 used to reidentify an identified or identifiable individual or be associated with  
9 an individual; or device that identifies or is linked or reasonably linkable to an  
10 individual or household; and

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

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

17 (C) contractually obligates any recipients of the data to satisfy the  
18 criteria set forth in subdivisions (A) and (B) of this subdivision (16). comply  
19 with all provisions of this subchapter.

20 (20) “Derived data” means data that is created by the derivation of  
21 information, data, assumptions, correlations, inferences, predictions, or

1 conclusions from facts, evidence, or another source of information or data  
2 about a consumer’s device.

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

5 (22) “First party” means a consumer-facing controller with which the  
6 consumer intends or expects to interact.

7 (23) “First-party advertising” means processing by a first party of its  
8 own first-party data for the purposes of advertising and marketing and is  
9 carried out:

10 (A) through direct communications with a consumer, such as direct  
11 mail, email, or text message communications;

12 (B) in a physical location operated by the first party; or

13 (C) through the display or presentation of an advertisement on the  
14 first party’s own website, application, or its other online content.

15 (24) “First-party data” means personal data collected directly from a  
16 consumer or by a first party in compliance with this subchapter, including  
17 based on a visit by the consumer to or use by the consumer of a website, a  
18 physical location, or an online service operated by the first party.

19 (1725) “Gender-affirming health care services” has the same meaning as  
20 in 1 V.S.A. § 150.

1           (1826) “Gender-affirming health data” means any personal data  
2           concerning a past, present, or future effort made by a consumer to seek, or a  
3           consumer’s receipt of, gender-affirming health care services, including:  
4           (A) precise geolocation data that is used for determining a  
5           consumer’s attempt to acquire or receive gender-affirming health care services;  
6           (B) efforts to research or obtain gender-affirming health care  
7           services; and  
8           (C) any gender-affirming health data that is derived from nonhealth  
9           information.  
10          (27) “Genetic data” means any data, regardless of its format, that results  
11          from the analysis of a biological sample of an individual, or from another  
12          source enabling equivalent information to be obtained, and concerns genetic  
13          material, including deoxyribonucleic acids (DNA), ribonucleic acids (RNA),  
14          genes, chromosomes, alleles, genomes, alterations or modifications to DNA or  
15          RNA, single nucleotide polymorphisms (SNPs), epigenetic markers,  
16          uninterpreted data that results from analysis of the biological sample or other  
17          source, and any information extrapolated, derived, or inferred therefrom.  
18          (1928) “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 (29) “Health care facility” has the same meaning as in 18 V.S.A. §  
4 9432.20

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

7 (2131) “Identified or identifiable individual” means an individual who  
8 can be readily identified, directly or indirectly, including by reference to an  
9 identifier such as a name, an identification number, precise geolocation data, or  
10 an online identifier.

11 (2232) “Institution of higher education” means any individual who, or  
12 school, board, association, limited liability company, or corporation that, is  
13 licensed or accredited to offer one or more programs of higher learning leading  
14 to one or more degrees.

15 (33) “Marketing measurement” means measuring and reporting on  
16 marketing performance or media performance by the controller, including  
17 processing personal data for measurement and reporting of frequency,  
18 attribution, and performance, provided that such measurement data is not  
19 processed or transferred for any other purpose.23

1           (34) “Mental health facility” means any health care facility in which at  
2           least 70 percent of the health care services provided in the facility are mental  
3           health services.

4           (35) “Minor” means any consumer who is younger than 18 years of  
5           age.~~24~~

6           (36) “Neural data” means information that is collected through  
7           biosensors and that could be processed to infer or predict mental states.

8           (37) “Nonprofit organization” means any organization that is qualified  
9           for tax exempt status under I.R.C. § 501(c)(3), 501(c)(4), 501(c)(6), or  
10           501(c)(12), or any corresponding internal revenue code of the United States, as  
11           may be amended.

12           (38) “Nonpublic personal information” has the same meaning as in 15  
13           U.S.C. § 6809.~~25~~

14           (39) “Patient-identifying information” has the same meaning as in  
15           42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

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

19           (2641)(A) “Personal data” means any information, including derived  
20           data and unique identifiers, that is linked or reasonably linkable, alone or in  
21           combination with other information, to an identified or identifiable individual

1 [or to a device that identifies, is linked to, or is reasonably linkable to one or](#)  
2 [more identified or identifiable individuals in a household.](#)

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

5 ~~(2742)~~(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 that reveals the past or present physical location of a consumer  
9 or device that identifies or is linked or reasonably linkable to one or more  
10 consumers with precision and accuracy within a radius of 1,7850 feet.

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

12 (i) the content of communications;

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

15 (iii) a photograph, or metadata associated with a photograph or  
16 video, that cannot be linked to an individual; or

17 ~~(iiiiv)~~ data generated by equipment used by a utility company.

18 ~~(2843)~~ “Process” or “processing” means any operation or set of  
19 operations performed, whether by manual or automated means, on personal  
20 data or on sets of personal data, such as the collection, use, storage, disclosure,  
21 analysis, deletion, ~~or~~ modification, or otherwise handling of personal data.

1           (2944) “Processor” means a person who processes personal data on  
2           behalf of:

3                   (A) a controller.;

4                   (B) another processor; or

5                   (C) a federal, state, tribal, or local government entity.

6           (3045) “Profiling” means any form of automated processing performed  
7           on personal data to evaluate, analyze, or predict personal aspects ~~related to an~~  
8           identified or identifiable, including an individual’s economic situation, health,  
9           personal preferences, interests, reliability, behavior, location, ~~or~~ movements, or  
10           identifying characteristics.

11           (3146) “Protected health information” has the same meaning as in  
12           HIPAA.

13           (3247) “Pseudonymous data” means personal data that cannot be  
14           attributed to a specific individual without the use of additional information,  
15           provided the additional information is kept separately and is subject to  
16           appropriate technical and organizational measures to ensure that the personal  
17           data ~~is~~are not attributed to an identified or identifiable individual.

18           (3348)(A) “Publicly available information” means information that:

19                   (Ai) is ~~lawfully~~ made available through federal, state, or local  
20           government records or to the general public from widely distributed media; or

1                    (Bii) a controller has a reasonable basis to believe that the  
2                    consumer has lawfully made available to the general public.

3                    (B) “Publicly available information” does not include:<sup>34</sup>

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

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

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

10                    (iv) an inference that is generated from the information described  
11                    in subdivision (ii) or (iii) of this subdivision (48)(B);

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

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

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

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

1                   (ix) intimate images, authentic or computer-generated, known to  
2 be nonconsensual.

3                   (49) “Reproductive or sexual health care” means any health care-related  
4 services or products rendered or provided concerning a consumer’has the same  
5 meaning as “reproductive system or sexual well-being, including any such  
6 service or product rendered or provided concerning: health care services” in 1  
7 V.S.A. § 150(c)(1).

8                   ~~(A) an individual health condition, status, disease, diagnosis,~~  
9 ~~diagnostic test or treatment;~~

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

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

12                   ~~(D) a use or purchase of a medication, including a medication used or~~  
13 ~~purchased for the purposes of an abortion, a bodily function, vital sign, or~~  
14 ~~symptom;~~

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

16                   ~~(F) an abortion, including medical or nonmedical services, products,~~  
17 ~~diagnostics, counseling, or follow-up services for an abortion.~~

18  
19                   (3550) “Reproductive or sexual health data” means any personal data  
20 concerning an effort made by a consumer to seek, or a consumer’s receipt of,  
21 reproductive or sexual health care.

1           (3651) “Reproductive or sexual health facility” means any health care  
2           facility in which at least 70 percent of the health care-related services or  
3           products rendered or provided in the facility are reproductive or sexual health  
4           care.

5           (3752)(A) “Sale of personal data” means the exchange of a consumer’s  
6           personal data by the controller to a third party for monetary or other valuable  
7           consideration.

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

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

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

13                   (iii) the disclosure or transfer of personal data to an affiliate of the  
14                  controller;

15                   (iv) the disclosure, with the consumer’s consent, of personal data  
16                  where the consumer directs the controller to disclose the personal data or  
17                  intentionally uses the controller to interact with a third party; or

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

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

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

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

5 (C) As used in subdivision (B) of this subdivision (52), “control” or  
6 “controlled” means: ~~38~~

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

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

11 (iii) the power to exercise controlling influence over the  
12 management of a company.

13 (53) “Sensitive data” means personal data that ~~includes:~~

14 (A) reveals a consumer’s government-issued identifier, such as a  
15 Social Security number, passport number, state identification card, or driver’s  
16 license number, that is not required by law to be publicly displayed;

17 ~~(A) data revealing~~ (B) reveals a consumer’s racial or ethnic origin,  
18 national origin, citizenship or immigration status, religious or philosophical  
19 beliefs, mental or physical health condition ~~or~~, diagnosis, ~~sex life, sexual~~  
20 ~~orientation, or citizenship or immigration status;~~ disability or treatment, status  
21 as pregnant, income level or indebtedness, or union membership;

1           (C) reveals a consumer’s sexual orientation, sex life, sexuality, or  
2           status as transgender or non-binary;

3           (D) reveals a consumer’s status as a victim of a crime;

4           (E) is a consumer’s tax return and account number, financial account  
5           log-in, financial account, debit card number, or credit card number in  
6           combination with any required security or access code, password, or  
7           credentials allowing access to an account;

8           ~~(B)~~ is consumer health data;

9           ~~(C) the processing of genetic or biometric data for the purpose of~~  
10          ~~uniquely identifying an individual;~~

11          (G) is collected and analyzed concerning consumer health data that  
12          describes or reveals a past, present, or future mental or physical health  
13          condition, treatment, disability, or diagnosis, including pregnancy, to the extent  
14          the personal data is used by the controller for a purpose other than to identify a  
15          specific consumer’s physical or mental health condition or diagnosis;

16          (H) is biometric or genetic data or information derived therefrom;

17          ~~(D) personal data~~ (I) is collected from a ~~known child~~ consumer who a  
18          controller knew or should have known is a minor;

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

20          ~~(F) an individual’s~~ (J) is precise geolocation data;

21          (K) are keystrokes;

1           (L) is driving behavior;

2           (M) is neural data; or

3           (N) are the online activities of a consumer over time and across  
4 ~~nonaffiliated~~ devices, websites ~~or~~, online applications, and mobile applications,  
5 that do not share common branding, or data generated by, profiling performed  
6 on such data.

7           (3954)(A) “Targeted advertising” means displaying or presenting an  
8 online advertisements to a consumer ~~where~~ or to a device identified by a unique  
9 persistent identifier, if the advertisement is selected based, ~~on personal data~~  
10 ~~obtained or inferred from that consumer’s activities over time and across~~  
11 ~~nonaffiliated websites or online applications to predict the consumer’s in whole~~  
12 or in part, on known or predicted preferences, characteristics, behavior, or  
13 interests associated with the consumer or a device identified by a unique  
14 persistent identifier.

15           (B) “Targeted advertising” ~~does not include~~: displaying or presenting  
16 an online advertisement for a product or service based on the ~~context~~ previous  
17 interaction of a consumer or a device identified by a unique persistent  
18 identifier with such product or service on a website or online service that does  
19 not share common branding with the website or online service displaying or  
20 presenting the advertisement, and marketing measurement related to such  
21 advertisements.

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

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

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

7 ~~(iv) processing personal data solely to measure or report~~  
8 ~~advertising frequency, performance, or reach.~~

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

10 (i) first-party advertising; or

11 (ii) contextual advertising.

12 (4055) “Third party” means a person, public authority, agency, or body,  
13 other than the consumer, controller, or processor or an affiliate of the processor  
14 or the controller.

15 (4156) “Trade secret” has the same meaning as in section 4601 of this  
16 title.

17 (57)(A) “Unique persistent identifier” means a technologically created  
18 identifier to the extent that such identifier is reasonably linkable to a consumer  
19 or a device that identifies or is linked or reasonably linkable to one or more  
20 consumers, including device identifiers, internet protocol addresses, cookies,  
21 beacons, pixel tags, mobile ad identifiers or similar technology customer

1 numbers, unique pseudonyms, user aliases, telephone numbers, or other forms  
2 of persistent or probabilistic identifiers that are linked or reasonably linkable to  
3 one or more consumers or devices.

4 (B) “Unique persistent identifier” does not include an identifier  
5 assigned by a controller for the sole purpose of giving effect to the exercise of  
6 affirmative consent or opt out by a consumer with respect to the collection or  
7 processing of personal data or otherwise limiting the collection or processing  
8 of personal data.

9 (58) “Victim services organization” means a nonprofit organization that  
10 is established to provide services to victims or witnesses of child abuse,  
11 domestic violence, human trafficking, sexual assault, violent felony, or  
12 stalking.

13 § 24165b. APPLICABILITY

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

18 (1) controlled or processed the personal data of not fewer than  
19 ~~100~~35,000 consumers, excluding personal data controlled or processed solely  
20 for the purpose of completing a payment transaction; ~~or~~

1           (2) ~~controlled or processed the personal data of not fewer than 25,000~~  
2 ~~consumers and derived more than 25 percent of the person's gross revenue~~  
3 ~~from the sale of personal data.~~ consumers' sensitive data, excluding personal  
4 data controlled or processed solely for the purposes of completing a payment  
5 transaction; or

6  
7           (3) sold the personal data of consumers.

8           **(b) Health data applicability.** ~~(b)~~ Section 24262415k of this title subchapter  
9 and the provisions of this subchapter concerning consumer health data and  
10 consumer health data controllers apply to a person that conducts business in  
11 this State or a person that produces products or services that are targeted to  
12 residents of this State.

13 § 24175c. EXEMPTIONS

14           (a) ~~Except as provided in subsection (c) of this section, this~~ This subchapter  
15 shall does not apply to any:

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

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

21           (3) ~~nonprofit organization;~~

- 1 ~~(4) institution of higher education;~~
- 2 ~~(5) national securities association that is registered under 15 U.S.C. 78o-~~
- 3 ~~3 of the Securities Exchange Act of 1934, as may be amended;~~
- 4 ~~(6) financial institution or data subject to Title V of the Gramm-Leach-~~
- 5 ~~Bliley Act, Pub. L. No. 106-102, and regulations adopted to implement that~~
- 6 ~~act;~~
- 7 ~~(7) covered entity or business associate, as defined in 45 C.F.R.~~
- 8 ~~§ 160.103;~~
- 9 ~~(8) tribal nation government organization; or~~
- 10 ~~(9) air carrier, as:~~
- 11 ~~(A) defined in 49 U.S.C. § 40102, as may be amended; and~~
- 12 ~~(B) regulated under the Federal Aviation Act of 1958, 49 U.S.C.~~
- 13 ~~§ 40101 et seq. and the Airline Deregulation Act of 1978, 49 U.S.C. § 41713,~~
- 14 ~~as may be amended.~~
- 15 ~~(b) The following information, data, and activities are exempt from this~~
- 16 ~~chapter:~~
- 17 1) in the ordinary course of its operation, a federal, state, tribal, or local
- 18 government entity or an instrumentality of the State;
- 19 (2) protected health information under HIPAA;
- 20 (3) patient-identifying information, for purposes of 42 U.S.C. § 290DD-
- 21 2;

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

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

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

13           ~~(3) identifiable private information;~~

14           C) information that is deidentified in accordance with the  
15 requirements for deidentification set forth in 45 C.F.R. § 164.514 and that is  
16 derived from individually identifiable health information as described in  
17 HIPAA; and

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

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

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

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

9 ~~(B) that is otherwise information collected as part of human subjects~~  
10 ~~research pursuant to the good clinical practice guidelines issued by the~~  
11 ~~International Council for Harmonisation of Technical Requirements for~~  
12 ~~Pharmaceuticals for Human Use;~~ activities that are subject to the protections  
13 provided in 21 C.F.R. Parts 50 (FDA clinical investigations protection of  
14 human subjects) and 56 (FDA clinical investigations institutional review  
15 boards); or

16 ~~(4) information that identifies a consumer in connection with the~~  
17 ~~protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal~~  
18 ~~data used or shared in research, as defined in 45 C.F.R. § 164.501, that is C)~~  
19 research conducted in accordance with the standards requirements set forth in  
20 this subdivision and in subdivisions (3A) and (B) of this subdivision; (a)(6)  
21 or otherwise research conducted in accordance with applicable law;

1 ~~(7) 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);~~<sup>5</sup>

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

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

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

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

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

1 ~~(9) information used for public health activities and purposes as~~  
2 ~~authorized by HIPAA, community health activities, and population health~~  
3 ~~activities;~~

4 10) information processed or maintained solely in connection with, and  
5 for the purpose of, enabling notice of an emergency to persons that an  
6 individual specifies;

7 ~~(10) the~~11) any activity that involves collection,  
8 ~~maintenance~~maintaining, disclosure, ing, sale~~selling, communication,~~ or use  
9 ~~of any personal~~using information bearing on ~~for the purpose of evaluating a~~  
10 consumer's credit-worthiness, credit standing, credit capacity, character,  
11 general reputation, personal characteristics, or mode of living ~~by~~ if done strictly  
12 in accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C.  
13 § 1681 et seq., 1681x, as may be amended, by:

14 ~~(A) a consumer reporting agency, furnisher, or user that provides~~  
15 ~~information for use in a consumer report, and by a user of a consumer report,~~  
16 ~~but only to the extent that such activity is regulated by and authorized under~~  
17 ~~the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., as may be amended;~~

18 (B) a person who furnishes information to a consumer reporting  
19 agency under 15 U.S.C. § 1681s-2 (responsibilities of furnishers of  
20 information for use in a consumer reporting agencies); or

1           (C) a person who uses a consumer report as provided in 15 U.S.C.  
2 § 1681b(a)(3) (permissible purposes of consumer reports);  
3           ~~(1112) personal data information~~ collected, processed, sold, or disclosed  
4 under and in ~~compliance~~accordance with: the following laws and regulations:  
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. data that is subject to L. No. 92-181, as~~  
8 ~~may be amended;~~  
9           ~~(12) personal data regulated by~~ the Family Educational Rights and  
10 Privacy Act, 20 U.S.C. § 1232g, ~~as may be amended;~~and regulations adopted  
11 to implement that act;  
12           (C) data that is subject to the Airline Deregulation Act, Pub. L. No.  
13 95-504, only to the extent that an air carrier collects information related to  
14 prices, routes, or services, and only to the extent that the provisions of the  
15 Airline Deregulation Act preempt this subchapter;  
16           (D) data that is subject to the Farm Credit Act, Pub. L. No. 92-181, as  
17 may be amended; and  
18           (E) data that is subject to federal policy under 21 U.S.C. § 830  
19 (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           18 U.S.C. § 1843(k);

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

11           (16) a third-party administrator, as that term is defined in the Third Party  
12           Administrator Rule adopted pursuant to 18 V.S.A. § 9417;

13           (17) personal data of a victim or witness of child abuse, domestic  
14           violence, human trafficking, sexual assault, violent felony, or stalking that a  
15           victim services organization collects, processes, or maintains in the course of  
16           its operation;

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

19           (19) information that is processed for purposes of compliance,  
20           enrollment or degree verification, or research services by a nonprofit

1 organization that is established to provide enrollment data reporting services  
2 on behalf of postsecondary schools as that term is defined in 16 V.S.A. § 176;

3 (20) noncommercial activity of:

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

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

9 (C) a nonprofit organization that provides programming to radio or  
10 television networks; or

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

12 ~~(13)~~ 21) data processed or maintained:

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

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

19 (C) that is necessary to retain to administer benefits for another

1 individual relating to the individual who is the subject of the information  
2 pursuant to subdivision (12) of this subsection (ba) and used for the purposes  
3 of administering such benefits; and.

4 ~~(14) personal data collected, processed, sold, or disclosed in relation to~~  
5 ~~price, route, or service, as such terms are used in the Federal Aviation Act of~~  
6 ~~1958, 49 U.S.C. § 40101 et seq., as may be amended, and the Airline~~  
7 ~~Deregulation Act of 1978, 49 U.S.C. § 41713, as may be amended.~~

8 (eb) Controllers, processors, and consumer health data controllers that  
9 comply with the verifiable parental consent requirements of COPPA shall be  
10 deemed compliant with any obligation to obtain parental consent pursuant to  
11 this subchapter.

12 ~~§ 24185d. CONSUMER PERSONAL DATA RIGHTS; COMPLIANCE BY~~  
13 ~~CONTROLLERS;~~

14 ~~APPEALS~~

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

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

19 (2) correct inaccuracies in the consumer's personal data, taking into  
20 account the nature of the personal data and the purposes of the processing of  
21 the consumer's personal data;

1           (3) delete personal data provided by, or obtained about, the consumer  
2 unless retention of the personal data is required by law;

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

8           (5) obtain from the controller a list of the third parties to which such  
9 controller has sold the consumer’s personal data or, if such controller does not  
10 maintain a list of the third parties to which such controller has sold the  
11 consumer’s personal data, a list of all third parties to which such controller has  
12 sold personal data, provided the controller shall not be required to reveal any  
13 trade secret;

14           (56) opt out of the processing of the personal data for purposes of:

15           (A) targeted advertising;

16           (B) the sale of personal data, ~~except as provided in subsection~~  
17 2420(b) of this title; or; and

18           (C) profiling in furtherance of ~~solely~~any automated decisions that  
19 produce legal or similarly significant effects concerning the consumer; and

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

4           (A) question the result of such profiling;

5           (B) be informed of the reason that such profiling resulted in such  
6 decision;

7           (C) review the consumer’s personal data that were processed for the  
8 purposes of such profiling, and

9           (D) if the profiling decision concerned housing, taking into account  
10 the nature of the personal data and the purposes for which such personal data  
11 were processed, allow the consumer to correct any incorrect personal data that  
12 were processed for the purposes of such profiling and have the profiling  
13 decision reevaluated based on the corrected personal data.

14           (b) Exercising consumer rights.

15           ~~(b)~~(1) A consumer may exercise rights under this section by a secure  
16 and reliable means established by the controller and described to the consumer  
17 in the controller’s privacy notice pursuant to subsection 2415e(c) of this  
18 subchapter.

19           (2)(A) ~~A consumer may designate an authorized agent in accordance~~  
20 ~~with section 2419 of this title to exercise the rights of the consumer to opt out~~  
21 ~~of the processing of the consumer’s personal data for purposes of subdivision~~

1 ~~(a)(5) of this section on behalf of the consumer.~~ another person to act on the  
2 consumer's behalf as the consumer's authorized agent for the purpose of  
3 exercising the consumer's rights pursuant to subdivisions (a)(1) and (a)(6) of  
4 this section.

5 (B) The consumer may designate an authorized agent by means of an  
6 internet link, browser setting, browser extension, global device setting, or other  
7 technology that enables the consumer to exercise the consumer's right pursuant  
8 to subdivision (A) of this subdivision (2).

9 (C) A controller shall comply with an opt-out request received from  
10 an 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 (3) In the case of processing personal data of a ~~known~~ consumer who:

14 (A) a controller has actual knowledge, or willfully disregards, is a  
15 child, the parent or legal guardian may exercise the consumer rights on the  
16 child's behalf.; and

17 ~~(4B) In the case of processing personal data concerning a consumer is~~  
18 subject to a guardianship, conservatorship, or other protective arrangement, the  
19 guardian or the conservator of the consumer may exercise the rights on the  
20 consumer's behalf.

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

4           (1) ~~(A)~~ Timeline to respond. A controller:

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

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

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

17           (3) Cost of information.

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

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

5           (C) ~~The~~A controller bears the burden of demonstrating the manifestly  
6           unfounded, excessive, or repetitive nature of the request.

7           (4) Authentication of request.

8           (A) If a controller is unable to authenticate a request to exercise any  
9           of the rights afforded under subdivisions (a)(1)–(45) of this section using  
10           commercially reasonable efforts, the controller shall not be required to comply  
11           with a request to initiate an action pursuant to this section and shall provide  
12           notice to the consumer that the controller is unable to authenticate the request  
13           to exercise the right or rights until the consumer provides additional  
14           information reasonably necessary to authenticate the consumer and the  
15           consumer’s request to exercise the right or rights.

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

19           (C) If a controller denies an opt-out request because the controller  
20           believes the request is fraudulent, the controller shall send a notice to the  
21           person who made the request disclosing that the controller believes the request

1 is fraudulent, why the controller believes the request is fraudulent, and that the  
2 controller shall not comply with the request.

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

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

11 (B) opting the consumer out of the processing of the personal data for  
12 any purpose except for those exempted pursuant to the provisions of this  
13 subchapter.

14 (d) Appeals.

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

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

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

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

8 ~~§ 2419. AUTHORIZED AGENTS AND CONSUMER OPT-OUT~~

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

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

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

1       (e) Disclosure of certain information. A controller, in response to a request  
2 from a consumer to exercise the consumer’s rights pursuant to subdivision  
3 (a)(1) of this section shall not disclose but instead inform the consumer or the  
4 person exercising such right on behalf of the consumer, with sufficient  
5 particularity, that the controller has collected the consumer’s:

6           (1) Social Security number;

7           (2) driver’s license number, state identification card number, or other  
8 government-issued identification number;

9           (3) financial account number;

10          (4) health insurance identification number or medical identification  
11 number;

12          (5) account password;

13          (6) security question or answer thereto; or

14          (7) biometric data.

15       ~~§ 2420.2415e. – DUTIES OF CONTROLLERS’ DUTIES; SALE OF~~  
16 ~~PERSONAL DATA TO~~

17 ~~THIRD PARTIES; NOTICE AND DISCLOSURE TO~~

18 ~~CONSUMERS; CONSUMER OPT-OUT~~

19       (a) Data collection and processing. ~~(a)~~ A controller:

20           (1) shall limit the collection and processing of personal data to what is  
21 adequate, relevant, and reasonably necessary in relation to the purposes for

1 which the data is processed, as disclosed to the consumer; and proportionate to  
2 provide or maintain:

3 ~~(2) except as otherwise provided in this chapter, shall not process~~  
4 ~~personal data for purposes that are neither reasonably necessary to, nor~~  
5 ~~compatible with, the disclosed purposes for which the personal data is~~  
6 ~~processed, as disclosed to the consumer, unless the controller obtains the~~  
7 ~~consumer's consent;~~

8 A) a specific product or service requested by the consumer to whom  
9 the data pertains; and

10 (B) a communication, that is not an advertisement, by the controller  
11 to the consumer that is reasonably anticipated within the context of the  
12 relationship between the controller and the consumer;

13 (2) may process or transfer the personal data of a consumer collected  
14 pursuant to subdivision (1) of this subsection to provide first-party advertising  
15 or targeted advertising to the consumer, unless:

16 (A) the personal data is sensitive data;

17 (B) the consumer has opted out of targeted advertising pursuant to  
18 subdivision 2415c(a)(6) of this subchapter; or

19 (C) the controller knew or willfully disregards that the consumer is a  
20 minor;

1           (3) shall establish, implement, and maintain reasonable administrative,  
2           technical, and physical data security practices to protect the confidentiality,  
3           integrity, and accessibility of personal data appropriate to the volume and  
4           nature of the personal data at issue; including disposing of personal data in  
5           accordance with a retention schedule that requires the deletion of personal data  
6           when the data is required to be deleted by law or is no longer necessary for the  
7           purpose for which the data was collected or processed;

8           (4) shall not collect or process sensitive data concerning a consumer  
9           ~~without obtaining the consumer's consent or, in the case of~~ except when the  
10           processing of is strictly necessary to provide or maintain a specific product or  
11           service requested by the consumer to whom the sensitive data ~~concerning a~~  
12           ~~known child, without processing the data in accordance with COPPA~~ pertains;

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

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

1 (7) shall not process the personal data of a consumer for the purposes of  
2 targeted advertising, or sell the consumer’s personal data, ~~without the~~  
3 ~~consumer’s consent, under circumstances where a controller has actual~~  
4 ~~knowledge, and if the controller knew or willfully disregards,~~ that the consumer  
5 ~~is at least 13 years of age but younger than 16 years of age; and a minor;~~

6 (8) shall not ~~sell sensitive data; and~~

7 (9) shall not discriminate against a consumer for exercising any of the  
8 consumer rights contained in this subchapter, including denying goods or  
9 services, charging different prices or rates for goods or services, or providing a  
10 different level of quality of goods or services to the consumer.

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

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

14 (2) prohibit a controller from offering a different price, rate, level,  
15 quality, or selection of goods or services to a consumer, including offering  
16 goods or services for no fee if the offering is in connection with a consumer’s  
17 voluntary participation in a bona fide loyalty, rewards, premium features,  
18 discounts, or club card program; provided that the selling of personal data is  
19 not a condition of participation in the program.

20 (c) Privacy notice. ~~(e)~~ A controller shall provide consumers with a  
21 reasonably accessible, clear, and meaningful privacy notice that includes:

- 1           (1) the categories of personal data processed by the controller;
- 2           (2) the purpose for processing personal data;
- 3           (3) how consumers may exercise their consumer rights, including how a  
4 consumer may appeal a controller’s decision with regard to the consumer’s  
5 request;
- 6           (4) the categories of personal data that the controller shares with third  
7 parties, if any;
- 8           (5) the categories of third parties, if any, with which the controller  
9 shares personal data; and
- 10          (6) an active email address or other online mechanism that the consumer  
11 may use to contact the controller.
- 12          (d) Targeted advertising. If a controller sells personal data to third parties  
13 or processes personal data for targeted advertising, the controller shall clearly  
14 and conspicuously disclose the selling or processing, as well as the manner in  
15 which a consumer may exercise the right to opt out of the selling or processing.
- 16          (e) Accessing consumer rights.
- 17           (1) A controller shall:
- 18           (A) establish, and shall describe in a privacy notice, one or more  
19 secure and reliable means for consumers to submit a request to exercise their  
20 consumer rights pursuant to this subchapter-; and

1           (B) not require a consumer to create a new account in order to  
2           exercise consumer rights but may require a consumer to use an existing  
3           account.

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

5           (A) take into account the ways in which consumers normally interact  
6           with the controller, the need for secure and reliable communication of the  
7           requests, and the ability of the controller to verify the identity of the consumer  
8           making the request.:

9           ~~(3) A controller shall not require a consumer to create a new account~~  
10           ~~in order to exercise consumer rights but may require a consumer to use an~~  
11           ~~existing account.~~

12           ~~(4)(A) The means shall include:~~

13           B(i) providing a clear and conspicuous link on the controller’s  
14           website to ~~an~~ web page that enables a consumer, or an agent of the consumer,  
15           to opt out of the targeted advertising or sale of the consumer’s personal data;  
16           and

17           (iiC) not later than January 1, 2026~~7~~, allowing a consumer to opt out  
18           of any processing of the consumer’s personal data for the purposes of targeted  
19           advertising, or any sale of the personal data, through an opt-out preference  
20           signal sent to the controller with the consumer’s consent indicating the

1 consumer's intent to opt out of any of the processing or sale, by a platform,  
2 technology, or other mechanism that shall:

3 (Ii) not unfairly disadvantage another controller;

4 (Hii) not make use of a default setting, but rather require the  
5 consumer to make an affirmative, freely given, and unambiguous choice to opt  
6 out of any processing of the consumer's personal data pursuant to this

7 subchapter;

8 (Hiii) be consumer-friendly and easy to use by the average  
9 consumer;

10 (IViv) be as consistent as possible with any other similar platform,  
11 technology, or mechanism required by any federal or State law or regulation;

12 and

13 (Vv) enable the controller to accurately determine whether the  
14 consumer is a resident of this State and whether the consumer has made a  
15 legitimate request to opt out of any sale of the consumer's personal data or  
16 targeted advertising.

17 (B3) If a consumer's decision to opt out of any processing of the  
18 consumer's personal data for the purposes of targeted advertising, or any sale  
19 of the personal data, through an opt-out preference signal sent in accordance  
20 with the provisions of subdivision (A2)(C) of this subdivision (e)(4)  
21 conflicts with the consumer's existing controller-specific privacy setting or

1 voluntary participation in a controller’s bona fide loyalty, rewards, premium  
2 features, discounts, or club card program, the controller shall comply with the  
3 consumer’s opt-out preference signal but may notify the consumer of the  
4 conflict and provide to the consumer the choice to confirm the controller-  
5 specific privacy setting or participation in the program.

6 (54) If a controller responds to a consumer opt-out requests received  
7 pursuant to subdivision (42)(AC) of this subsection by informing the consumer  
8 of a charge for the use of any product or service, the controller shall present the  
9 terms of any financial incentive offered pursuant to subdivisecion (b)(2) of  
10 this section for the retention, use, sale, or sharing of the consumer’s personal  
11 data.

12 § 24215f. PROCESSORS’ DUTIES; CONTRACTS BETWEEN

13 CONTROLLERS AND PROCESSORS

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

17 (1) taking into account the nature of processing and the information  
18 available to the processor, by appropriate technical and organizational  
19 measures, to the extent reasonably practicable, to fulfill the controller’s  
20 obligation to respond to consumer rights requests;

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

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

9           **(b) Contractual terms.**

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

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

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

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

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

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

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

10           (E) make available to the controller upon the reasonable request of  
11           the controller, all information in the processor’s possession necessary to  
12           demonstrate the processor’s compliance with this subchapter.

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

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

19           (d) Processors performing as controllers.

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

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

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

10          (4) If a processor begins, alone or jointly with others, determining the  
11 purposes and means of the processing of personal data, the processor is a  
12 controller with respect to the processing and may be subject to an enforcement  
13 action under section 24252415j of this title subchapter.

14 § 2422.2415g. ~~CONTROLLERS’~~ DATA PROTECTION ASSESSMENTS;  
15 DISCLOSURE TO

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           consumers;

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

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

12                   (D) other substantial injury to consumers; 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 any data protection assessment the  
2 use of de-identified 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) Disclosure to Attorney General.

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

10          (2) The Attorney General may evaluate the data protection assessment  
11 for compliance with the responsibilities set forth in this subchapter.

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

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

18           (d) Assessment efficiency and applicability.

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

1           (e2) If a controller conducts a data protection assessment for the purpose  
2 of 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           (f3) Data protection assessment requirements shall apply to processing  
8 activities created or generated after July 1, 20256, and are not retroactive.

9       § ~~2423~~2415h. DE-IDENTIFIED AND PSEUDONYMOUS DATA; DATA  
10 CONTROLLERS' DUTIES; EXCEPTIONS; APPLICABILITY OF  
11 CONSUMERS' RIGHTS; DISCLOSURE AND OVERSIGHT

12       (a) Requirements. (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 subchapter.

19       (b) Limitations. This subchapter 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; or

4           ~~(e3) This chapter shall not be construed to~~ require a controller or  
5 processor to comply with an authenticated consumer rights request if the  
6 controller:

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

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

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

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

1 c) Oversight when disclosing.(e) A controller that discloses pseudonymous  
2 data or de-identified data shall exercise reasonable oversight to monitor  
3 compliance with any contractual commitments to which the pseudonymous  
4 data or de-identified data is subject and shall take appropriate steps to address  
5 any breaches of those contractual commitments.

6 § 24242415i. CONSTRUCTION OF ~~CONTROLLERS' AND~~  
7 ~~PROCESSORS'~~

8 —————DUTIES

9 (a) Generally. This subchapter shall not be construed to restrict a  
10 controller's, processor's, or consumer health data controller's ability to:

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

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

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

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

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

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

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

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

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

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

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

18           (B) the expected benefits of the research outweigh the privacy risks;

19           and

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

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

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

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

11           (B) under the responsibility of a professional subject to  
12 confidentiality obligations under federal, state, or local law; ~~or~~

13           ~~(b13) The obligations imposed on controllers, processors, or consumer~~  
14 ~~health data controllers under this chapter shall not restrict a controller's,~~  
15 ~~processor's, or consumer health data controller's ability to collect, use, or~~  
16 ~~retain data for internal use to:~~

17           ~~(1A)~~ conduct internal research to develop, improve, or repair  
18 products, services, or technology;

19           ~~(2B)~~ effectuate a product recall;

20           ~~(3C)~~ identify and repair technical errors that impair existing or  
21 intended functionality; or

1           (4D) perform internal operations that are reasonably aligned with the  
2 expectations of the consumer or reasonably anticipated based on the  
3 consumer’s existing relationship with the controller or consumer health data  
4 controller, or are otherwise compatible with processing data in furtherance of  
5 the provision of a product or service specifically requested by a consumer or  
6 the performance of a contract to which the consumer is a party.

7           (eb) Evidentiary privilege.

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

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

16           (3) Nothing in this subchapter modifies 2020 Acts and Resolves No.  
17 166, Sec. 14 or authorizes the use of facial recognition technology by law  
18 enforcement.d)

19           (c) Third parties.

20           (1) A controller, processor, or consumer health data controller that  
21 discloses personal data to a processor or third-party controller pursuant to this

1 subchapter shall not be deemed to have violated this subchapter if the  
2 processor or third-party controller that receives and processes the personal data  
3 violates this subchapter, provided, at the time the disclosing controller,  
4 processor, or consumer health data controller disclosed the personal data, the  
5 disclosing controller, processor, or consumer health data controller did not  
6 have actual knowledge that the receiving processor or third-party controller  
7 would violate this subchapter.

8 (2) A third-party controller or processor receiving personal data from a  
9 controller, processor, or consumer health data controller in compliance with  
10 this subchapter is not in violation of this subchapter for the transgressions of  
11 the controller, processor, or consumer health data controller from which the  
12 third-party controller or processor receives the personal data.

13 (ed) Clarifications. This subchapter shall not be construed to:

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

16 (A) to freedom of speech or freedom of the press guaranteed in the  
17 First Amendment to the United States U.S. Constitution; or

18 (B) under 12 V.S.A. § 1615;

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

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

6           ~~(f)~~ Personal data processing.

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

10           (A) reasonably necessary and proportionate to the purposes listed in  
11 this section; and

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

14           (2)(A) Personal data collected, used, or retained pursuant to  
15 subdivisecton ~~(b)~~(13) of this section shall, where applicable, take into  
16 account the nature and purpose or purposes of the collection, use, or retention.

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

1           ~~(g3)~~ If a controller or consumer health data controller processes personal  
2 data pursuant to an exemption in this section, the controller or consumer health  
3 data controller bears the burden of demonstrating that the processing qualifies  
4 for the exemption and complies with the requirements ~~in~~of this subsection ~~(f)~~  
5 of this section.

6           ~~(h4)~~ Processing personal data for the purposes expressly identified in  
7 this section shall not solely make a legal entity a controller or consumer health  
8 data controller with respect to the processing.

9   § ~~24252415j~~. ~~ENFORCEMENT BY ATTORNEY GENERAL; NOTICE OF~~  
10 ~~VIOLATION; CURE PERIOD; REPORT; PENALTY~~

11           ~~(a)~~ The Attorney General shall have exclusive authority to enforce  
12 violations of this chapter.

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

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

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

3 ~~(A) the number of notices of violation the Attorney General has~~  
4 ~~issued;~~

5 ~~(B) the nature of each violation;~~

6 ~~(C) the number of violations that were cured during the available~~  
7 ~~cure period; and~~

8 ~~(D) any other matter the Attorney General deems relevant for the~~  
9 ~~purposes of the report.~~

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

13 ~~(1) the number of violations;~~

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

15 ~~(3) the nature and extent of the controller's or processor's processing~~  
16 ~~activities;~~

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

18 ~~(5) the safety of persons or property;~~

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

21 ~~(7) the sensitivity of the data.~~

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

4 ~~(e) Subjection to the exception in subsection (f) of this section, aa) A~~  
5 violation of the requirements of this subchapter shall constitute an unfair and  
6 deceptive act in commerce in violation of section 2453 of this title and shall be  
7 enforced solely by the Attorney General, provided that a consumer private  
8 right of action under subsection 2461(b) of this title shall not apply to the  
9 violation.

10 ~~(f) The Attorney General shall provide guidance to controllers and~~  
11 ~~processors for compliance with the terms of the Vermont Data Privacy Act.~~  
12 ~~Any processor or controller that, in the opinion of the Attorney General,~~  
13 ~~materially complies with the guidance provided by the Attorney General shall~~  
14 ~~not constitute an unfair and deceptive act in commerce.~~

15 b) The Attorney General has the same authority to adopt rules to implement  
16 the provisions of this subchapter and to conduct civil investigations, enter into  
17 assurances of discontinuance, bring civil actions, and take other enforcement  
18 actions as provided under chapter 63, subchapter 1 of this title.

19 (c) Annually, on or before February 1, the Attorney General shall submit a  
20 report to the General Assembly disclosing:

1 (A1) the number of notices of violation pursuant to this subchapter that  
2 the Attorney General has issued;

3 (B2) the nature of each violation;

4 (C3) the number of violations that resulted in an enforcement action  
5 being taken;

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

7 (D5) any other matter the Attorney General deems relevant for the  
8 purposes of the report.

9 § 24262415k. CONSUMER HEALTH DATA PRIVACY

10 (a) Except as provided in subsections (b) and (c) section 2415i of this  
11 sectionsubchapter and subsections 24175c(b) and (c) of this titlesubchapter, no  
12 person shall:

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

16 (2) provide any processor with access to consumer health data unless the  
17 person and processor comply with section 24215f of this title;subchapter; or

18 (3) use a geofence to establish a virtual boundary that is within 1,7850  
19 feet of any health care facility, including any mental health facility or  
20 reproductive or sexual health facility, for the purpose of identifying, tracking,

1 collecting data from, or sending any notification to a consumer regarding the  
2 consumer’s consumer health data; ~~or.~~

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

5 Sec. 2. DATA PRIVACY UNIT CREATION; ATTORNEY GENERAL;

6 APPROPRIATION

7 (a) The Office of the Attorney General shall establish a data privacy unit  
8 for the purpose of regulating and enforcing 9 V.S.A. chapter 61A (Vermont  
9 Data Privacy and Online Surveillance Act). The data privacy unit shall be  
10 composed of at least two attorneys and one investigator.

11 ~~(b) Notwithstanding section 2416 of this title,~~ b) In fiscal year 2027,  
12 \$650,000.00 is appropriated from the General Fund to the Office of the  
13 Attorney General for the purpose of creating and funding the data privacy unit  
14 pursuant to subsection (a) of this section, and the provisions of sections 2415–  
15 2425 of this title, inclusive, concerning consumer health data and consumer  
16 health data controllers, apply to persons that conduct business in this state and  
17 persons that produce products or services that are targeted to residents of this  
18 state.

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

20 ~~(1) body, authority, board, bureau, commission, district or agency of this~~  
21 ~~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) institution of higher education;~~

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

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

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

12 ~~(7) tribal nation government organization; or~~

13 ~~(8) air carrier, as:~~

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

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

1 Sec. 23. EFFECTIVE DATE

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

3

4

5

6

7

8 (Committee vote: \_\_\_\_\_)

9

10

\_\_\_\_\_  
Representative

11

\_\_\_\_\_  
FOR THE COMMITTEE

DRAFTABLE