

1 TO THE HOUSE OF REPRESENTATIVES:

2 The Committee on Commerce and Economic Development to which was
3 referred House Bill No. 121 entitled “An act relating to enhancing consumer
4 privacy” respectfully reports that it has considered the same and recommends
5 that the bill be amended by striking out all after the enacting clause and
6 inserting in lieu thereof the following:

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

8 CHAPTER 61A: VERMONT DATA PRIVACY ACT

9 § 2415. DEFINITIONS

10 As used in this chapter:

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

14 (B) As used in subdivision (1)(A) of this section, “control” or
15 “controlled” means:

16 (i) ownership of, or the power to vote, more than fifty percent of
17 the outstanding shares of any class of voting security of a company;

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

20 (iii) the power to exercise controlling influence over the
21 management of a company.

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

5 (3)(A) “Biometric data” means data generated by automatic
6 measurements of an individual's biological characteristics, such as a
7 fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns
8 or characteristics that are used to identify a specific individual.

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

10 (i) a digital or physical photograph;

11 (ii) an audio or video recording; or

12 (iii) any data generated from a digital or physical photograph, or
13 an audio or video recording, unless the data is generated to identify a specific
14 individual.

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

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

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

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

1 (C) “Consent” does not include:

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

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

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

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

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

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

18 (9) “COPPA” means the Children's Online Privacy Protection Act of
19 1998, 15 USC 6501 et seq., and the regulations, rules, guidance, and
20 exemptions adopted pursuant to the act, as the act and regulations, rules,
21 guidance, and exemptions may be amended from time to time.

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

2 (11) “Dark pattern”

3 (A) means a user interface designed or manipulated with the
4 substantial effect of subverting or impairing user autonomy, decision-making,
5 or choice; and

6 (B) includes any practice the Federal Trade Commission refers to as a
7 “dark pattern.”

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

14 (13) “De-identified data” means data that cannot reasonably be used to
15 infer information about, or otherwise be linked to, an identified or identifiable
16 individual, or a device linked to the individual, if the controller that possesses
17 the data:

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

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

1 (C) contractually obligates any recipients of the data to satisfy the
2 criteria set forth in subdivisions (A) and (B) of this subdivision (13).

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

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

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

12 (17) “Nonprofit organization” means any organization that is exempt
13 from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of
14 the Internal Revenue Code of 1986,1 or any subsequent corresponding internal
15 revenue code of the United States, as amended from time to time.

16 (18)(A) “Personal data” means any information that is linked or
17 reasonably linkable to an identified or identifiable individual.

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

20 (19)(A) “Precise geolocation data” means information derived from
21 technology, including global positioning system level latitude and longitude

1 coordinates or other mechanisms, that directly identifies the specific location
2 of an individual with precision and accuracy within a radius of one thousand
3 seven hundred fifty feet.

4 (B) “Precise geolocation data” does not include the content of
5 communications or any data generated by or connected to advanced utility
6 metering infrastructure systems or equipment for use by a utility.

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

11 (21) “Processor” means an individual who, or legal entity that, processes
12 personal data on behalf of a controller.

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

17 (23) “Protected health information” has the same meaning as provided
18 in HIPAA.

19 (24) “Pseudonymous data” means personal data that cannot be attributed
20 to a specific individual without the use of additional information, provided the
21 additional information is kept separately and is subject to appropriate technical

1 and organizational measures to ensure that the personal data is not attributed to
2 an identified or identifiable individual.

3 (25) “Publicly available information” means information that:

4 (A) is lawfully made available through federal, state, or municipal
5 government records or widely distributed media; and

6 (B) a controller has a reasonable basis to believe a consumer has
7 lawfully made available to the general public.

8 (26)(A) “Sale of personal data” means the exchange of personal data for
9 monetary or other valuable consideration by the controller to a third party.

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

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

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

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

17 (iv) the disclosure of personal data where the consumer directs the
18 controller to disclose the personal data or intentionally uses the controller to
19 interact with a third party;

20 (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 (27) “Sensitive data” means personal data that includes:

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

12 (B) the processing of genetic or biometric data for the purpose of
13 uniquely identifying an individual;

14 (C) personal data collected from a known child; or

15 (D) precise geolocation data.

16 (28)(A) “Targeted advertising” means displaying advertisements to a
17 consumer where the advertisement is selected based on personal data obtained
18 or inferred from that consumer's activities over time and across nonaffiliated
19 Internet web sites or online applications to predict the consumer's preferences
20 or interests.

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

1 (i) advertisements based on activities within a controller's own
2 Internet web sites or online applications;

3 (ii) advertisements based on the context of a consumer's current
4 search query, visit to an Internet web site, or online application;

5 (iii) advertisements 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 (29) “Third party” means an individual or legal entity, such as a public
10 authority, agency, or body, other than the consumer, controller, or processor or
11 an affiliate of the processor or the controller.

12 (30) “Trade secret” has the same meaning as provided in section 4601 of
13 this title.

14 § 2416. APPLICABILITY

15 This chapter applies to a person that conducts business in this State or a
16 person that produces products or services that are targeted to residents of this
17 State and that during the preceding calendar year:

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

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

4 § 2417. EXEMPTIONS

5 (a) This chapter does not apply to:

6 (1) a national securities association that is registered under 15 USC 78o-
7 3 of the Securities Exchange Act of 1934, as amended from time to time;

8 (2) a financial institution or data subject to Title V of the Gramm-Leach-
9 Bliley Act, 15 USC 6801 et seq.; or

10 (3) a covered entity or business associate, as defined in 45 CFR 160.103.

11 (b) The following information and data are exempt from the provisions of
12 this chapter:

13 (1) protected health information under HIPAA;

14 (2) patient-identifying information for purposes of 42 USC 290dd-2;

15 (3) identifiable private information for purposes of the federal policy for
16 the protection of human subjects under 45 CFR 46;

17 (4) identifiable private information that is otherwise information
18 collected as part of human subjects research pursuant to the good clinical
19 practice guidelines issued by the International Council for Harmonization of
20 Technical Requirements for Pharmaceuticals for Human Use;

1 (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56,
2 or personal data used or shared in research, as defined in 45 CFR 164.501, that
3 is conducted in accordance with the standards set forth in this subdivision and
4 subdivisions (3) and (4) of this subsection, or other research conducted in
5 accordance with applicable law;

6 (6) information and documents created for purposes of the Health Care
7 Quality Improvement Act of 1986, 42 USC 11101 et seq.;

8 (7) patient safety work product for purposes of section 19a-127o and the
9 Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as
10 amended from time to time;

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

14 (9) information originating from and intermingled to be
15 indistinguishable with, or information treated in the same manner as,
16 information exempt under this subsection that is maintained by a covered
17 entity or business associate, program or qualified service organization, as
18 specified in 42 USC 290dd-2, as amended from time to time;

19 (10) information used for public health activities and purposes as
20 authorized by HIPAA, community health activities, and population health
21 activities;

1 (11) the collection, maintenance, disclosure, sale, communication, or use
2 of any personal information bearing on a consumer's credit worthiness, credit
3 standing, credit capacity, character, general reputation, personal characteristics
4 or mode of living by a consumer reporting agency, furnisher, or user that
5 provides information for use in a consumer report, and by a user of a consumer
6 report, but only to the extent that the activity is regulated by and authorized
7 under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from
8 time to time;

9 (12) personal data collected, processed, sold, or disclosed in compliance
10 with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as
11 amended from time to time;

12 (13) personal data regulated by the Family Educational Rights and
13 Privacy Act, 20 USC 1232g et seq., as amended from time to time;

14 (14) personal data collected, processed, sold, or disclosed in compliance
15 with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time;

16 (15) data processed or maintained:

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

20 (B) as the emergency contact information of an individual under this
21 chapter, used for emergency contact purpose; or

1 (C) that is necessary to retain to administer benefits for another
2 individual relating to the individual who is the subject of the information under
3 subdivision (1) of this subsection and used for the purposes of administering
4 the benefits; and

5 (16) personal data collected, processed, sold, or disclosed in relation to
6 price, route, or service, as the terms are used in the Airline Deregulation Act,
7 49 USC 40101 et seq., as amended from time to time, by an air carrier subject
8 to the act, to the extent a provision of this chapter is preempted by the Airline
9 Deregulation Act, 49 USC 41713, as amended from time to time.

10 (c) Controllers and processors that comply with the verifiable parental
11 consent requirements of COPPA shall be deemed compliant with any
12 obligation to obtain parental consent pursuant to this chapter.

13 § 2418. CONSUMER’S RIGHTS; COMPLIANCE BY CONTROLLERS;

14 APPEALS

15 (a) A consumer may:

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

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

8 (A) targeted advertising;

9 (B) the sale of personal data, except as provided in subsection
10 2420(b) of this title; or

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

13 (b)(1) A consumer may exercise rights under this section by a secure and
14 reliable means established by the controller and described to the consumer in
15 the controller's privacy notice.

16 (2) A consumer may designate an authorized agent in accordance with
17 section 2419 of this title to exercise the rights of the consumer to opt out of the
18 processing of the consumer's personal data for purposes of subdivision (a)(5)
19 of this section on behalf of the consumer.

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

1 (4) In the case of processing personal data concerning a consumer
2 subject to a guardianship, conservatorship, or other protective arrangement, the
3 guardian or the conservator of the consumer may exercise the rights on the
4 consumer's behalf.

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

8 (1)(A) A controller shall respond to the consumer without undue delay,
9 but not later than forty-five days after receipt of the request.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4 § 2419. AUTHORIZED AGENTS AND CONSUMER OPT-OUT

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

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

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

17 § 2420. CONTROLLERS' DUTIES; SALE OF PERSONAL DATA TO

18 THIRD PARTIES; NOTICE AND DISCLOSURE TO CONSUMERS;

19 CONSUMER OPT-OUT

20 (a) A controller:

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

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

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

13 (4) shall not process sensitive data concerning a consumer without
14 obtaining the consumer's consent, or, in the case of the processing of sensitive
15 data concerning a known child, without processing the data in accordance with
16 COPPA;

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

19 (6) shall provide an effective mechanism for a consumer to revoke the
20 consumer's consent under this section that is at least as easy as the mechanism
21 by which the consumer provided the consumer's consent and, upon revocation

1 of the consent, cease to process the data as soon as practicable, but not later
2 than fifteen days after the receipt of the request;

3 (7) shall not process the personal data of a consumer for purposes of
4 targeted advertising, or sell the consumer's personal data without the
5 consumer's consent, under circumstances where a controller has actual
6 knowledge, and wilfully disregards, that the consumer is at least thirteen years
7 of age but younger than sixteen years of age; and

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

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

20 (c) A controller shall provide consumers with a reasonably accessible,
21 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 electronic mail address or other online mechanism that the
11 consumer may use to contact the controller.
12 (d) If a controller sells personal data to third parties or processes personal
13 data for targeted advertising, the controller shall clearly and conspicuously
14 disclose the processing, as well as the manner in which a consumer may
15 exercise the right to opt out of the processing.
16 (e)(1) A controller shall establish, and shall describe in a privacy notice,
17 one or more secure and reliable means for consumers to submit a request to
18 exercise their consumer rights pursuant to this chapter.
19 (2) The means shall take into account the ways in which consumers
20 normally interact with the controller, the need for secure and reliable

1 communication of the requests, and the ability of the controller to verify the
2 identity of the consumer making the request.

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

6 (4) The means shall include:

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

11 (ii) not later than January 1, 2026, allowing a consumer to opt out
12 of any processing of the consumer's personal data for the purposes of targeted
13 advertising, or any sale of the personal data, through an opt-out preference
14 signal sent to the controller with the consumer's consent indicating the
15 consumer's intent to opt out of any the processing or sale, by a platform,
16 technology, or other mechanism that shall:

17 (I) not unfairly disadvantage another controller;

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

1 (III) be consumer-friendly and easy to use by the average
2 consumer;

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

6 (V) enable the controller to accurately determine whether the
7 consumer is a resident of this State and whether the consumer has made a
8 legitimate request to opt out of any sale of the consumer's personal data or
9 targeted advertising.

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

20 (5) If a controller responds to consumer opt-out requests received
21 pursuant to subdivision (4)(A) of this subsection by informing the consumer of

1 a charge for the use of any product or service, the controller shall present the
2 terms of any financial incentive offered pursuant to subsection (b) of this
3 section for the retention, use, sale, or sharing of the consumer's personal data.

4 § 2421. PROCESSORS' DUTIES; CONTRACTS BETWEEN

5 CONTROLLERS AND PROCESSORS

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

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

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

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

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

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

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

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

11 (B) at the controller's direction, delete or return all personal data to
12 the controller as requested at the end of the provision of services, unless
13 retention of the personal data is required by law;

14 (C) upon the reasonable request of the controller, make available to
15 the controller all information in its possession necessary to demonstrate the
16 processor's compliance with the obligations in this chapter;

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

20 (E) allow, and cooperate with, reasonable assessments by the
21 controller or the controller's designated assessor, or the processor may arrange

1 for a qualified and independent assessor to conduct an assessment of the
2 processor's policies and technical and organizational measures in support of the
3 obligations under this chapter using an appropriate and accepted control
4 standard or framework and assessment procedure for the assessments.

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

7 (c) This section shall not be construed to relieve a controller or processor
8 from the liabilities imposed on the controller or processor by virtue of the
9 controller's or processor's role in the processing relationship, as described in
10 this chapter.

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

14 (2) A person who is not limited in the person's processing of personal
15 data pursuant to a controller's instructions, or who fails to adhere to the
16 instructions, is a controller and not a processor with respect to a specific
17 processing of data.

18 (3) A processor that continues to adhere to a controller's instructions
19 with respect to a specific processing of personal data remains a processor.

20 (4) If a processor begins, alone or jointly with others, determining the
21 purposes and means of the processing of personal data, the processor is a

1 controller with respect to the processing and may be subject to an enforcement
2 action under section 2425 of this title.

3 § 2422. CONTROLLERS' DATA PROTECTION ASSESSMENTS;

4 DISCLOSURE TO ATTORNEY GENERAL

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

8 (1) the processing of personal data for the purposes of targeted
9 advertising;

10 (2) the sale of personal data;

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

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

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

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

19 (D) other substantial injury to consumers; and

20 (4) the processing of sensitive data.

1 (b)(1) Data protection assessments conducted pursuant to subsection (a) of
2 this section shall identify and weigh the benefits that may flow, directly and
3 indirectly, from the processing to the controller, the consumer, other
4 stakeholders, and the public against the potential risks to the rights of the
5 consumer associated with the processing, as mitigated by safeguards that can
6 be employed by the controller to reduce the risks.

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

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

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

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

19 (4) To the extent any information contained in a data protection
20 assessment disclosed to the Attorney General includes information subject to

1 attorney-client privilege or work product protection, the disclosure shall not
2 constitute a waiver of the privilege or protection.

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

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

11 (f) Data protection assessment requirements shall apply to processing
12 activities created or generated after July 1, 2024, and are not retroactive.

13 § 2423. DE-IDENTIFIED AND PSEUDONYMOUS DATA;

14 CONTROLLERS' DUTIES; EXCEPTIONS; APPLICABILITY OF
15 CONSUMERS' RIGHTS; DISCLOSURE AND OVERSIGHT

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

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

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

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

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

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

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

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

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

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

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

20 (d) The rights afforded under subdivisions 2418(a)(1) to (4) of this title
21 shall not apply to pseudonymous data in cases where the controller is able to

1 demonstrate that any information necessary to identify the consumer is kept
2 separately and is subject to effective technical and organizational controls that
3 prevent the controller from accessing the information.

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

9 § 2424. CONSTRUCTION OF CONTROLLERS' AND PROCESSORS'

10 DUTIES

11 (a) This chapter shall not be construed to restrict a controller's or
12 processor's ability to:

13 (1) comply with federal, state, or municipal laws, ordinances, or
14 regulations;

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

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

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

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

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

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

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

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

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

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

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

20 and

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

4 (11) assist another controller, processor, or third party with any of the
5 obligations under this chapter; 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.

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

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

18 (2) effectuate a product recall;

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

1 (4) 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 are otherwise
4 compatible with processing data in furtherance of the provision of a product or
5 service specifically requested by a consumer or the performance of a contract
6 to which the consumer is a party.

7 (c)(1) The obligations imposed on controllers or processors under this
8 chapter shall not apply where compliance by the controller or processor with
9 this chapter would violate an evidentiary privilege under the laws of this State.

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

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

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

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

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

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

10 (B) under 12 V.S.A. § 1615; or

11 (2) apply to any person's processing of personal data in the course of the
12 person's purely personal or household activities.

13 (f)(1) Personal data processed by a controller pursuant to this section may
14 be processed to the extent that the processing is:

15 (A) reasonably necessary and proportionate to the purposes listed in
16 this section; and

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

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

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

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

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

12 § 2425. ENFORCEMENT BY ATTORNEY GENERAL; NOTICE OF
13 VIOLATION; CURE PERIOD; REPORT; PENALTY

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

16 (b)(1) During the period beginning on July 1, 2024, and ending on
17 December 31, 2025, the Attorney General shall, prior to initiating any action
18 for a violation of any provision of this chapter, issue a notice of violation to the
19 controller if the Attorney General determines that a cure is possible.

1 (2) If the controller fails to cure the violation within sixty days of receipt
2 of the notice of violation, the Attorney General may bring an action pursuant to
3 this section.

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

6 (A) the number of notices of violation the Attorney General has
7 issued;

8 (B) the nature of each violation;

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

11 (4) any other matter the Attorney General deems relevant for the
12 purposes of the report.

13 (c) Beginning on January 1, 2026, the Attorney General may, in
14 determining whether to grant a controller or processor the opportunity to cure
15 an alleged violation described in subsection (b) of this section, consider:

16 (1) the number of violations;

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

18 (3) the nature and extent of the controller's or processor's processing
19 activities;

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

21 (5) the safety of persons or property; and

1 (6) whether the alleged violation was likely caused by human or
2 technical error.

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

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

11 Sec. 2. 9 V.S.A. chapter 62 is amended to read:

12 CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

13 Subchapter 1. General Provisions

14 § 2430. DEFINITIONS

15 As used in this chapter:

16 (1) “Biometric identifier” means unique biometric data generated from
17 measurements or technical analysis of an individual’s biological
18 characteristics, including a fingerprint, voiceprint, retina, iris, or other unique
19 biological characteristics, which is used to identify a specific individual.

1 (2)(A) “Brokered personal information” means one or more of the
2 following computerized data elements about a consumer, if categorized or
3 organized for dissemination to third parties:

4 (i) name;

5 (ii) address;

6 (iii) date of birth;

7 (iv) place of birth;

8 (v) mother’s maiden name;

9 (vi) ~~unique biometric data generated from measurements or~~
10 ~~technical analysis of human body characteristics used by the owner or licensee~~
11 ~~of the data to identify or authenticate the consumer, the as a fingerprint, retina~~
12 ~~or iris image, or other unique physical representation or digital representation~~
13 ~~of biometric data~~ biometric identifier;

14 (vii) name or address of a member of the consumer’s immediate
15 family or household;

16 (viii) Social Security number or other government-issued
17 identification number; or

18 (ix) other information that, alone or in combination with the other
19 information sold or licensed, would allow a reasonable person to identify the
20 consumer with reasonable certainty.

1 (B) “Brokered personal information” does not include publicly
2 available information to the extent that it is related to a consumer’s business or
3 profession.

4 ~~(2)~~(3) “Business” means a commercial entity, including a sole
5 proprietorship, partnership, corporation, association, limited liability company,
6 or other group, however organized and whether or not organized to operate at a
7 profit, including a financial institution organized, chartered, or holding a
8 license or authorization certificate under the laws of this State, any other state,
9 the United States, or any other country, or the parent, affiliate, or subsidiary of
10 a financial institution, but does not include the State, a State agency, any
11 political subdivision of the State, or a vendor acting solely on behalf of, and at
12 the direction of, the State.

13 ~~(3)~~(4) “Consumer” means an individual residing in this State.

14 ~~(4)~~(5)(A) “Data broker” means a business, or unit or units of a business,
15 separately or together, that knowingly collects and sells or licenses to third
16 parties the brokered personal information of a consumer with whom the
17 business does not have a direct relationship.

18 (B) Examples of a direct relationship with a business include if the
19 consumer is a past or present:

20 (i) customer, client, subscriber, user, or registered user of the
21 business’s goods or services;

1 (ii) employee, contractor, or agent of the business;

2 (iii) investor in the business; or

3 (iv) donor to the business.

4 (C) The following activities conducted by a business, and the
5 collection and sale or licensing of brokered personal information incidental to
6 conducting these activities, do not qualify the business as a data broker:

7 (i) developing or maintaining third-party e-commerce or
8 application platforms;

9 (ii) providing 411 directory assistance or directory information
10 services, including name, address, and telephone number, on behalf of or as a
11 function of a telecommunications carrier;

12 (iii) providing publicly available information related to a
13 consumer's business or profession; or

14 (iv) providing publicly available information via real-time or near-
15 real-time alert services for health or safety purposes.

16 (D) The phrase "sells or licenses" does not include:

17 (i) a one-time or occasional sale of assets of a business as part of a
18 transfer of control of those assets that is not part of the ordinary conduct of the
19 business; or

20 (ii) a sale or license of data that is merely incidental to the
21 business.

1 ~~(5)~~(6)(A) “Data broker security breach” means an unauthorized
2 acquisition or a reasonable belief of an unauthorized acquisition of more than
3 one element of brokered personal information maintained by a data broker
4 when the brokered personal information is not encrypted, redacted, or
5 protected by another method that renders the information unreadable or
6 unusable by an unauthorized person.

7 (B) “Data broker security breach” does not include good faith but
8 unauthorized acquisition of brokered personal information by an employee or
9 agent of the data broker for a legitimate purpose of the data broker, provided
10 that the brokered personal information is not used for a purpose unrelated to
11 the data broker’s business or subject to further unauthorized disclosure.

12 (C) In determining whether brokered personal information has been
13 acquired or is reasonably believed to have been acquired by a person without
14 valid authorization, a data broker may consider the following factors, among
15 others:

16 (i) indications that the brokered personal information is in the
17 physical possession and control of a person without valid authorization, the as
18 a lost or stolen computer or other device containing brokered personal
19 information;

20 (ii) indications that the brokered personal information has been
21 downloaded or copied;

1 (iii) indications that the brokered personal information was used
2 by an unauthorized person, the as fraudulent accounts opened or instances of
3 identity theft reported; or

4 (iv) that the brokered personal information has been made public.

5 ~~(6)~~(7) “Data collector” means a person who, for any purpose, whether
6 by automated collection or otherwise, handles, collects, disseminates, or
7 otherwise deals with personally identifiable information, and includes the
8 State, State agencies, political subdivisions of the State, public and private
9 universities, privately and publicly held corporations, limited liability
10 companies, financial institutions, and retail operators.

11 ~~(7)~~(8) “Encryption” means use of an algorithmic process to transform
12 data into a form in which the data is rendered unreadable or unusable without
13 use of a confidential process or key.

14 ~~(8)~~(9) “License” means a grant of access to, or distribution of, data by
15 one person to another in exchange for consideration. A use of data for the sole
16 benefit of the data provider, where the data provider maintains control over the
17 use of the data, is not a license.

18 ~~(9)~~(10) “Login credentials” means a consumer’s user name or e-mail
19 address, in combination with a password or an answer to a security question,
20 that together permit access to an online account.

1 ~~(10)~~(11)(A) “Personally identifiable information” means a consumer’s
2 first name or first initial and last name in combination with one or more of the
3 following digital data elements, when the data elements are not encrypted,
4 redacted, or protected by another method that renders them unreadable or
5 unusable by unauthorized persons:

6 (i) a Social Security number;

7 (ii) a driver license or nondriver State identification card number,
8 individual taxpayer identification number, passport number, military
9 identification card number, or other identification number that originates from
10 a government identification document that is commonly used to verify identity
11 for a commercial transaction;

12 (iii) a financial account number or credit or debit card number, if
13 the number could be used without additional identifying information, access
14 codes, or passwords;

15 (iv) a password, personal identification number, or other access
16 code for a financial account;

17 (v) ~~unique biometric data generated from measurements or~~
18 ~~technical analysis of human body characteristics used by the owner or licensee~~
19 ~~of the data to identify or authenticate the consumer, the as a fingerprint, retina~~
20 ~~or iris image, or other unique physical representation or digital representation~~
21 ~~of biometric data~~ a biometric identifier;

1 (vi) genetic information; and

2 (vii)(I) health records or records of a wellness program or similar
3 program of health promotion or disease prevention;

4 (II) a health care professional’s medical diagnosis or treatment
5 of the consumer; or

6 (III) a health insurance policy number.

7 (B) “Personally identifiable information” does not mean publicly
8 available information that is lawfully made available to the general public from
9 federal, State, or local government records.

10 ~~(11)~~(12) “Record” means any material on which written, drawn, spoken,
11 visual, or electromagnetic information is recorded or preserved, regardless of
12 physical form or characteristics.

13 ~~(12)~~(13) “Redaction” means the rendering of data so that the data are
14 unreadable or are truncated so that no more than the last four digits of the
15 identification number are accessible as part of the data.

16 ~~(13)~~(14)(A) “Security breach” means unauthorized acquisition of
17 electronic data, or a reasonable belief of an unauthorized acquisition of
18 electronic data, that compromises the security, confidentiality, or integrity of a
19 consumer’s personally identifiable information or login credentials maintained
20 by a data collector.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

* * *

§ 2436. NOTICE OF DATA BROKER SECURITY BREACH

(a) Short title. This section shall be known as the Data Broker Security Breach Notice Act.

(b) Notice of breach.

(1) Except as otherwise provided in subsection (d) of this section, any data broker shall notify the consumer that there has been a data broker security breach following discovery or notification to the data broker of the breach.

Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency, as provided in subdivisions (3) and (4) of this subsection, or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) A data broker shall provide notice of a breach to the Attorney

General as follows:

(A)(i) The data broker shall notify the Attorney General of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 business days, consistent with the legitimate needs of the law enforcement agency, as provided in subdivision (3) and subdivision (4) of this subsection (b), after the data broker’s discovery

1 of the security breach or when the data broker provides notice to consumers
2 pursuant to this section, whichever is sooner.

3 (ii) If the date of the breach is unknown at the time notice is sent
4 to the Attorney General, the data broker shall send the Attorney General the
5 date of the breach as soon as it is known.

6 (iii) Unless otherwise ordered by a court of this State for good
7 cause shown, a notice provided under this subdivision (2)(A) shall not be
8 disclosed to any person other than the authorized agent or representative of the
9 Attorney General, a State’s Attorney, or another law enforcement officer
10 engaged in legitimate law enforcement activities without the consent of the
11 data broker.

12 (B)(i) When the data broker provides notice of the breach pursuant to
13 subdivision (1) of this subsection (b), the data broker shall notify the Attorney
14 General of the number of Vermont consumers affected, if known to the data
15 broker, and shall provide a copy of the notice provided to consumers under
16 subdivision (1) of this subsection (b).

17 (ii) The data broker may send to the Attorney General a second
18 copy of the consumer notice, from which is redacted the type of brokered
19 personal information that was subject to the breach, that the Attorney General
20 shall use for any public disclosure of the breach.

1 (3) The notice to a consumer required by this subsection shall be
2 delayed upon request of a law enforcement agency. A law enforcement agency
3 may request the delay if it believes that notification may impede a law
4 enforcement investigation or a national or Homeland Security investigation or
5 jeopardize public safety or national or Homeland Security interests. In the
6 event law enforcement makes the request for a delay in a manner other than in
7 writing, the data broker shall document the request contemporaneously in
8 writing and include the name of the law enforcement officer making the
9 request and the officer’s law enforcement agency engaged in the investigation.
10 A law enforcement agency shall promptly notify the data broker in writing
11 when the law enforcement agency no longer believes that notification may
12 impede a law enforcement investigation or a national or Homeland Security
13 investigation, or jeopardize public safety or national or Homeland Security
14 interests. The data broker shall provide notice required by this section without
15 unreasonable delay upon receipt of a written communication, which includes
16 facsimile or electronic communication, from the law enforcement agency
17 withdrawing its request for delay.

18 (4) The notice to a consumer required in subdivision (1) of this
19 subsection shall be clear and conspicuous. A notice to a consumer of a
20 security breach involving brokered personal information shall include a
21 description of each of the following, if known to the data broker:

1 (A) the incident in general terms;

2 (B) the type of brokered personal information that was subject to the
3 security breach;

4 (C) the general acts of the data broker to protect the brokered
5 personal information from further security breach;

6 (D) a telephone number, toll-free if available, that the consumer may
7 call for further information and assistance;

8 (E) advice that directs the consumer to remain vigilant by reviewing
9 account statements and monitoring free credit reports; and

10 (F) the approximate date of the data broker security breach.

11 (5) A data broker may provide notice of a security breach involving
12 brokered personal information to a consumer by one or more of the following
13 methods:

14 (A) written notice mailed to the consumer’s residence;

15 (B) electronic notice, for those consumers for whom the data broker
16 has a valid e-mail address, if:

17 (i) the data broker’s primary method of communication with the
18 consumer is by electronic means, the electronic notice does not request or
19 contain a hypertext link to a request that the consumer provide personal
20 information, and the electronic notice conspicuously warns consumers not to

1 provide personal information in response to electronic communications
2 regarding security breaches; or

3 (ii) the notice is consistent with the provisions regarding electronic
4 records and signatures for notices in 15 U.S.C. § 7001; or

5 (C) telephonic notice, provided that telephonic contact is made
6 directly with each affected consumer and not through a prerecorded message.

7 (c) Exception.

8 (1) Notice of a security breach pursuant to subsection (b) of this section
9 is not required if the data broker establishes that misuse of brokered personal
10 information is not reasonably possible and the data broker provides notice of
11 the determination that the misuse of the brokered personal information is not
12 reasonably possible pursuant to the requirements of this subsection. If the data
13 broker establishes that misuse of the brokered personal information is not
14 reasonably possible, the data broker shall provide notice of its determination
15 that misuse of the brokered personal information is not reasonably possible and
16 a detailed explanation for said determination to the Vermont Attorney General.
17 The data broker may designate its notice and detailed explanation to the
18 Vermont Attorney General as a trade secret if the notice and detailed
19 explanation meet the definition of trade secret contained in 1 V.S.A. §
20 317(c)(9).

1 (a) Annually, on or before January 31 following a year in which a person
2 meets the definition of data broker as provided in section 2430 of this title, a
3 data broker shall:

4 (1) register with the Secretary of State;

5 (2) pay a registration fee of \$100.00; and

6 (3) provide the following information:

7 (A) the name and primary physical, e-mail, and Internet addresses of
8 the data broker;

9 (B) ~~if the data broker permits~~ the method for a consumer to opt out of
10 the data broker's collection of brokered personal information, opt out of its
11 databases, or opt out of ~~certain~~ sales of data:

12 (i) the method for requesting an opt-out;

13 (ii) If the opt-out applies to only certain activities or sales, which
14 ones; and

15 (iii) whether the data broker permits a consumer to authorize a
16 third party to perform the opt-out on the consumer's behalf;

17 (C) ~~a statement specifying the data collection, databases, or sales~~
18 ~~activities from which a consumer may not opt out;~~

19 (D) ~~a statement whether the data broker implements a purchaser~~
20 ~~credentialing process;~~

1 ~~(E) the number of data broker security breaches that the data broker~~
2 ~~has experienced during the prior year, and if known, the total number of~~
3 ~~consumers affected by the breaches;~~

4 ~~(F) where the data broker has actual knowledge that it possesses the~~
5 ~~brokered personal information of minors, a separate statement detailing the~~
6 ~~data collection practices, databases, and sales activities, ~~and opt-out policies~~~~
7 ~~that are applicable to the brokered personal information of minors; and~~

8 ~~(G)~~(D) any additional information or explanation the data broker
9 chooses to provide concerning its data collection practices.

10 (b) A data broker that fails to register pursuant to subsection (a) of this
11 section is liable to the State for:

12 (1) a civil penalty of ~~\$50.00~~ \$100.00 for each day, ~~not to exceed a total~~
13 ~~of \$10,000.00 for each year,~~ it fails to register pursuant to this section;

14 (2) an amount equal to the fees due under this section during the period
15 it failed to register pursuant to this section; and

16 (3) other penalties imposed by law.

17 (c) A data broker that omits required information from its registration shall
18 file an amendment to include the omitted information within five business days
19 following notification of the omission and is liable to the State for a civil
20 penalty of \$1,000.00 per day for each day thereafter.

1 (3) A data broker shall clearly and conspicuously describe the opt-out
2 procedure in its annual registration and on its website.

3 (b) General opt-out.

4 (1) A consumer may request that all data brokers registered with the
5 State of Vermont honor an opt-out request by filing the request with the
6 Secretary of State.

7 (2) The Secretary of State shall develop an online form to facilitate the
8 general opt-out by a consumer and shall maintain a Data Broker Opt-Out List
9 of consumers who have requested a general opt-out, with the specific type of
10 opt-out.

11 (3) The Data Broker Opt-Out List shall contain the minimum amount of
12 information necessary for a data broker to identify the specific consumer
13 making the opt-out.

14 (4) Once every 31 days, any data broker registered with the State of
15 Vermont shall review the Data Broker Opt-Out List in order to comply with
16 the opt-out requests contained therein.

17 (5) Data contained in the Data Broker Opt-Out List shall not be used for
18 any purpose other than to effectuate a consumer's opt-out request.

19 (c) Credentialing.

1 (1) A data broker shall maintain reasonable procedures designed to
2 ensure that the brokered personal information it discloses is used for a
3 legitimate and legal purpose.

4 (2) These procedures shall require that prospective users of the
5 information identify themselves, certify the purposes for which the information
6 is sought, and certify that the information shall be used for no other purpose.

7 (3) A data broker shall make a reasonable effort to verify the identity of
8 a new prospective user and the uses certified by the prospective user prior to
9 furnishing the user brokered personal information.

10 (4) A data broker shall not furnish brokered personal information to any
11 person if it has reasonable grounds for believing that the consumer report will
12 not be used for a legitimate and legal purpose.

13 (d) Exemption. Nothing in this section applies to brokered personal
14 information that is regulated as a consumer report pursuant to the Fair Credit
15 Reporting Act, if the data broker is fully complying with the Fair Credit
16 Reporting Act.

17 Subchapter 6. Biometric Information

18 § 2449. PROTECTION OF BIOMETRIC INFORMATION

19 (a) Collection, use, and retention of biometric identifiers.

1 (1) A person shall not collect or retain a biometric identifier without first
2 providing clear and conspicuous notice pursuant to this section and providing a
3 mechanism to opt out of the subsequent use of a biometric identifier.

4 (2) A person providing notice pursuant to subdivision (1) of this
5 subsection shall include:

6 (A) a description of the biometric identifiers being collected or
7 retained;

8 (B) the specific purpose and length of term for which a biometric
9 identifier or biometric information is being collected, stored, or used;

10 (C) the third parties to which the biometric identifier may be sold,
11 leased, or otherwise disclosed to and the purpose of the disclosure; and

12 (D) the mechanism by which the consumer may opt out of the
13 subsequent use of the biometric identifier.

14 (3) A person who has collected or stored a consumer's biometric
15 identifier may not use, sell, lease, or otherwise disclose the biometric identifier
16 to another person if a consumer has exercised the consumer's right to opt out
17 of the subsequent use of a biometric identifier.

18 (4) A person who possesses a biometric identifier of a consumer:

19 (A) shall take reasonable care to guard against unauthorized access to
20 and acquisition of biometric identifiers that are in the possession or under the
21 control of the person;

1 (B) shall adopt a comprehensive information security program that
2 complies with section 2447 of this title; and

3 (C) may retain the biometric identifier not longer than is reasonably
4 necessary to:

5 (i) comply with a court order, statute, or public records retention
6 schedule specified under federal, state, or local law;

7 (ii) protect against or prevent actual or potential fraud, criminal
8 activity, claims, security threats, or liability; and

9 (iii) provide the services for which the biometric identifier was
10 collected or stored.

11 (5)(A) A person who collects or retains biometric identifiers shall
12 establish a retention schedule and guidelines for permanently destroying
13 biometric identifiers and biometric information when the initial purpose for
14 collecting or obtaining the identifiers or information has been satisfied or
15 within one year of the consumer’s last interaction with the person, whichever
16 occurs first.

17 (B) Absent a valid warrant or subpoena issued by a court of
18 competent jurisdiction, a person who possesses biometric identifiers or
19 biometric information shall comply with its established retention schedule and
20 destruction guidelines.

1 (6) A person who collects or stores a biometric identifier of a consumer
2 or obtains a biometric identifier of a consumer from a third party pursuant to
3 this section may not use or disclose it in a manner that is materially
4 inconsistent with the terms under which the biometric identifier was originally
5 provided without disclosing the new terms of use or disclosure and providing a
6 mechanism to opt out of the new use of the biometric identifier.

7 (7) Nothing in this section requires a person to provide notice to a
8 consumer if:

9 (A) the biometric identifier will be used solely to authenticate the
10 consumer for the purpose of securing the goods or services provided by the
11 business;

12 (B) the biometric identifier will not be leased or sold to any third
13 party; and

14 (C) the biometric identifier will only be disclosed to a third party for
15 the purpose of effectuating subdivision (A) of this subdivision (a)(7), and the
16 third party is contractually obligated to maintain the confidentiality of the
17 biometric identifier and to not further disclose the biometric identifier.

18 (b) Enforcement.

19 (1)(A) The Attorney General and State’s Attorney shall have authority
20 to investigate potential violations of this subchapter and to enforce, prosecute,
21 obtain, and impose remedies for a violation of this subchapter or any rules or

1 regulations made pursuant to this chapter as the Attorney General and State's
2 Attorney have under chapter 63 of this title. The Attorney General may refer
3 the matter to the State's Attorney in an appropriate case. The Superior Courts
4 shall have jurisdiction over any enforcement matter brought by the Attorney
5 General or a State's Attorney under this subsection.

6 (B) In determining appropriate civil penalties, the courts shall
7 consider each instance in which a person violates this subchapter with respect
8 to each consumer as a separate violation and shall base civil penalties on the
9 seriousness of the violation, the size and sophistication of the business
10 violating the subchapter, and the business's history of respecting or failing to
11 respect the privacy of consumers, with maximum penalties imposed where
12 appropriate.

13 (C) A person who possesses a biometric identifier of a consumer that
14 was not acquired in accordance with the requirements of this subchapter as of
15 the effective date of this law shall either obtain consent or delete the biometric
16 information within 180 days after enactment of this law or shall be liable for
17 \$10,000.00 per day thereafter until the business has complied with this
18 subdivision (1)(c).

19 (2) A consumer aggrieved by a violation of this subchapter or rules
20 adopted under this subchapter may bring an action in Superior Court for the
21 consumer's damages, injunctive relief, punitive damages, and reasonable costs

1 and attorney’s fees. The court, in addition, may issue an award for the greater
2 of the consumer’s actual damages or \$1,000.00 a negligent violation or
3 \$5,000.00 for a willful or reckless violation.

4 (c) Exclusions. Nothing in this chapter expands or limits the authority of a
5 law enforcement officer acting within the scope of the officer’s authority,
6 including the authority of a State law enforcement officer in executing lawful
7 searches and seizures.

8 Sec. 3. EFFECTIVE DATE

9 This act shall take effect on July 1, 2024.

10
11
12
13
14
15
16
17
18
19
20

(Committee vote: _____)

Representative _____
FOR THE COMMITTEE