

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) “Abortion” has the same meaning as in section 2492 of this title.

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

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

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

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

1 (iii) the power to exercise controlling influence over the
2 management of a company.

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

7 (4) “Biometric data” means personal data generated from the
8 technological processing of an individual’s unique biological, physical, or
9 physiological characteristics that is linked or reasonably linkable to an
10 individual, including:

11 (A) iris or retina scans;

12 (B) fingerprints;

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

14 (D) vein patterns;

15 (E) voice prints;

16 (F) gait or personally identifying physical movement or patterns;

17 (G) depictions, images, descriptions, or recordings; and

18 (H) data derived from any data in subdivision (G) of this subdivision

19 (4), to the extent that it would be reasonably possible to identify the specific
20 individual from whose biometric data the data has been derived.

21 (5) “Broker-dealer” has the same meaning as in 9 V.S.A. § 5102.

1 (6) “Business associate” has the same meaning as in HIPAA.

2 (7) “Child” has the same meaning as in COPPA.

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

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

8 (C) “Consent” does not include:

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

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

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

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

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

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

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

7 (12) “Consumer reporting agency” has the same meaning as in the Fair
8 Credit Reporting Act, 15 U.S.C. § 1681a(f);

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

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

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

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

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

1 (18) “Decisions that produce legal or similarly significant effects
2 concerning the consumer” means decisions made by the controller that result in
3 the provision or denial by the controller of financial or lending services,
4 housing, insurance, education enrollment or opportunity, criminal justice,
5 employment opportunities, health care services, or access to essential goods or
6 services.

7 (19) “De-identified data” means data that does not identify and cannot
8 reasonably be used to infer information about, or otherwise be linked to, an
9 identified or identifiable individual, or a device linked to the individual, if the
10 controller that possesses the data:

11 (A)(i) takes reasonable measures to ensure that the data cannot be
12 used to re-identify an identified or identifiable individual or be associated with
13 an individual or device that identifies or is linked or reasonably linkable to an
14 individual or household;

15 (ii) for purposes of this subdivision (A), “reasonable measures”
16 shall include the de-identification requirements set forth under 45 C.F.R.
17 § 164.514 (other requirements relating to uses and disclosures of protected
18 health information);

19 (B) publicly commits to process the data only in a de-identified
20 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 (19).

3 (20) “Financial institution”:

4 (A) as used in subdivision 2417(a)(12) of this title, has the same
5 meaning as in 15 U.S.C. § 6809; and

6 (B) as used in subdivision 2417(a)(14) of this title, has the same
7 meaning as in 8 V.S.A. § 11101.

8 (21) “Gender-affirming health care services” has the same meaning as in
9 1 V.S.A. § 150.

10 (22) “Gender-affirming health data” means any personal data
11 concerning a past, present, or future effort made by a consumer to seek, or a
12 consumer’s receipt of, gender-affirming health care services, including:

13 (A) precise geolocation data that is used for determining a
14 consumer’s attempt to acquire or receive gender-affirming health care services;

15 (B) efforts to research or obtain gender-affirming health care
16 services; and

17 (C) any gender-affirming health data that is derived from nonhealth
18 information.

19 (23) “Genetic data” means any data, regardless of its format, that results
20 from the analysis of a biological sample of an individual, or from another
21 source enabling equivalent information to be obtained, and concerns genetic

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

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

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

13 (26) “Heightened risk of harm to a minor” means processing the
14 personal data of a minor in a manner that presents a reasonably foreseeable risk
15 of:

16 (A) unfair or deceptive treatment of, or unlawful disparate impact on,
17 a minor;

18 (B) financial, physical, mental, emotional, or reputational injury to a
19 minor;

20 (C) unintended disclosure of the personal data of a minor; or

1 (D) any physical or other intrusion upon the solitude or seclusion, or
2 the private affairs or concerns, of a minor if the intrusion would be offensive to
3 a reasonable person.

4 (27) “HIPAA” means the Health Insurance Portability and
5 Accountability Act of 1996, Pub. L. No. 104-191, and any regulations
6 promulgated pursuant to the act, as may be amended.

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

11 (29) “Independent trust company” has the same meaning as in 8 V.S.A.
12 § 2401.

13 (30) “Investment adviser” has the same meaning as in 9 V.S.A. § 5102.

14 (31) “Mental health facility” means any health care facility in which at
15 least 70 percent of the health care services provided in the facility are mental
16 health services.

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

19 (33)(A) “Online service, product, or feature” means any service,
20 product, or feature that is provided online, except as provided in subdivision
21 (B) of this subdivision (33).

1 (B) “Online service, product, or feature” does not include:

2 (i) telecommunications service, as that term is defined in the
3 Communications Act of 1934, 47 U.S.C. § 153;

4 (ii) broadband internet access service, as that term is defined in
5 47 C.F.R. § 54.400 (universal service support); or

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

7 (34) “Patient identifying information” has the same meaning as in
8 42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

9 (35) “Patient safety work product” has the same meaning as in 42 C.F.R.
10 § 3.20 (patient safety organizations and patient safety work product).

11 (36)(A) “Personal data” means any information, including derived data
12 and unique identifiers, that is linked or reasonably linkable to an identified or
13 identifiable individual or to a device that identifies, is linked to, or is
14 reasonably linkable to one or more identified or identifiable individuals in a
15 household.

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

18 (37)(A) “Precise geolocation data” means personal data that accurately
19 identifies within a radius of 1,850 feet a consumer’s present or past location or
20 the present or past location of a device that links or is linkable to a consumer or
21 any data that is derived from a device that is used or intended to be used to

1 locate a consumer within a radius of 1,850 feet by means of technology that
2 includes a global positioning system that provides latitude and longitude
3 coordinates.

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 (38) “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 (39) “Processor” means a person who processes personal data on behalf
12 of a controller.

13 (40) “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 (41) “Protected health information” has the same meaning as in HIPAA.

18 (42) “Pseudonymous data” means personal data that cannot be attributed
19 to a specific individual without the use of additional information, provided the
20 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 (43) “Publicly available information” means information that:

4 (A) is lawfully made available through federal, state, or local
5 government records; or

6 (B) a controller has a reasonable basis to believe that the consumer
7 has lawfully made available to the general public through widely distributed
8 media.

9 (44) “Qualified service organization” has the same meaning as in 42
10 C.F.R. § 2.11 (confidentiality of substance use disorder patient records);

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

13 (46) “Reproductive or sexual health data” means any personal data
14 concerning a past, present, or future effort made by a consumer to seek, or a
15 consumer’s receipt of, reproductive or sexual health care.

16 (47) “Reproductive or sexual health facility” means any health care
17 facility in which at least 70 percent of the health care-related services or
18 products rendered or provided in the facility are reproductive or sexual health
19 care.

20 (48)(A) “Sale of personal data” means the sale, rent, release, disclosure,
21 dissemination, provision, transfer, or other communication, whether oral, in

1 writing, or by electronic or other means, of a consumer’s personal data by the
2 controller to a third party for monetary or other valuable consideration or
3 otherwise for a commercial purpose.

4 (B) For purposes of this subdivision (48), “commercial purpose”
5 means to advance a person’s commercial or economic interests, such as by
6 inducing another person to buy, rent, lease, join, subscribe to, provide, or
7 exchange products, goods, property, information, or services, or enabling or
8 effecting, directly or indirectly, a commercial transaction.

9 (C) “Sale of personal data” does not include:

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

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

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

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

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

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

1 (II) did not restrict to a specific audience; or
2 (vi) the disclosure or transfer of personal data to a third party as an
3 asset that is part of a merger, acquisition, bankruptcy or other transaction, or a
4 proposed merger, acquisition, bankruptcy, or other transaction, in which the
5 third party assumes control of all or part of the controller’s assets.

6 (49) “Sensitive data” means personal data that:

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

10 (B) reveals a consumer’s racial or ethnic origin, national origin,
11 citizenship or immigration status, religious or philosophical beliefs, or union
12 membership;

13 (C) reveals a consumer’s sexual orientation, sex life, sexuality, or
14 status as transgender or nonbinary;

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

16 (E) is financial information, including a consumer’s account number,
17 financial account log-in, financial account, debit card number, or credit card
18 number in combination with any required security or access code, password, or
19 credentials allowing access to an account;

20 (F) is consumer health data;

1 (G) is personal data collected and analyzed concerning consumer
2 health data or personal data that describes or reveals a past, present, or future
3 mental or physical health condition, treatment, disability, or diagnosis,
4 including pregnancy, to the extent the personal data is not used by the
5 controller to identify a specific consumer’s physical or mental health condition
6 or diagnosis;

7 (H) is biometric or genetic data;

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

9 (J) is a photograph, film, video recording, or other similar medium
10 that shows the naked or undergarment-clad private area of a consumer; or

11 (K) is precise geolocation data.

12 (50)(A) “Targeted advertising” means:

13 (i) except as provided in subdivision (ii) of this subdivision

14 (50)(A), the targeting of an advertisement to a consumer based on the

15 consumer’s activity with one or more businesses, distinctly branded websites,

16 applications, or services, other than the controller, distinctly branded website,

17 application, or service with which the consumer is intentionally interacting;

18 and

19 (ii) as used in section 2420 of this title, the targeting of an

20 advertisement to a minor based on the minor’s activity with one or more

21 businesses, distinctly branded websites, applications, or services, including

1 with the controller, distinctly branded website, application, or service with
2 which the minor is intentionally interacting.

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

4 (i) for targeted advertising to a consumer other than a minor, an
5 advertisement based on activities within a controller’s own commonly branded
6 website or online application;

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

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

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

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

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

17 (53) “Victim services organization” means a nonprofit organization that
18 is established to provide services to victims or witnesses of child abuse,
19 domestic violence, human trafficking, sexual assault, violent felony, or
20 stalking.

21 § 2416. APPLICABILITY

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

5 (1) controlled or processed the personal data of not fewer than 6,500
6 consumers, excluding personal data controlled or processed solely for the
7 purpose of completing a payment transaction; or

8 (2) controlled or processed the personal data of not fewer than 3,250
9 consumers and derived more than 20 percent of the person’s gross revenue
10 from the sale of personal data.

11 (b) Sections 2420, 2424, and 2428 of this title, and the provisions of this
12 chapter concerning consumer health data and consumer health data controllers
13 apply to a person that conducts business in this State or a person that produces
14 products or services that are targeted to residents of this State.

15 § 2417. EXEMPTIONS

16 (a) This chapter does not apply to:

17 (1) a federal, State, tribal, or local government entity in the ordinary
18 course of its operation;

19 (2) protected health information that a covered entity or business
20 associate processes in accordance with, or documents that a covered entity or
21 business associate creates for the purpose of complying with HIPAA;

1 (3) 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 (4) information that identifies a consumer in connection with:

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

8 (B) research on human subjects undertaken in accordance with good
9 clinical practice guidelines issued by the International Council for
10 Harmonisation of Technical Requirements for Pharmaceuticals for Human
11 Use;

12 (C) activities that are subject to the protections provided in 21 C.F.R.
13 parts 50 (FDA clinical investigations protection of human subjects) and 56
14 (FDA clinical investigations institutional review boards); or

15 (D) research conducted in accordance with the requirements set forth
16 in subdivisions (A) through (C) of this subdivision (a)(4) or otherwise in
17 accordance with applicable law;

18 (5) patient identifying information that is collected and processed in
19 accordance with 42 C.F.R. part 2 (confidentiality of substance use disorder
20 patient records);

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

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

7 (8) information that originates from, that is intermingled so as to be
8 indistinguishable from, or that is treated in the same manner as information
9 described in subdivisions (2)–(7) of this subsection that a covered entity,
10 business associate, or a qualified service organization program creates,
11 collects, processes, uses, or maintains in the same manner as is required under
12 the laws, regulations, and guidelines described in subdivisions (2)–(7) of this
13 subsection;

14 (9) information processed or maintained solely in connection with, and
15 for the purpose of, enabling:

16 (A) an individual’s employment or application for employment;

17 (B) an individual’s ownership of, or function as a director or officer
18 of, a business entity;

19 (C) an individual’s contractual relationship with a business entity;

20 (D) an individual’s receipt of benefits from an employer, including
21 benefits for the individual’s dependents or beneficiaries; or

1 (E) notice of an emergency to persons that an individual specifies;
2 (10) any activity that involves collecting, maintaining, disclosing,
3 selling, communicating, or using information for the purpose of evaluating a
4 consumer’s creditworthiness, credit standing, credit capacity, character,
5 general reputation, personal characteristics, or mode of living if done strictly in
6 accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C.
7 § 1681–1681x, as may be amended, by:

8 (A) a consumer reporting agency;

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

12 (C) a person who uses a consumer report as provided in 15 U.S.C.
13 § 1681b(a)(3) (permissible purposes of consumer reports);

14 (11) information collected, processed, sold, or disclosed under and in
15 accordance with the following laws and regulations:

16 (A) the Driver’s Privacy Protection Act of 1994, 18 U.S.C. § 2721–
17 2725;

18 (B) the Family Educational Rights and Privacy Act, 20 U.S.C.
19 § 1232g, and regulations adopted to implement that act;

20 (C) the Airline Deregulation Act, Pub. L. No. 95-504, only to the
21 extent that an air carrier collects information related to prices, routes, or

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

2 Act preempt this chapter;

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

4 (E) federal policy under 21 U.S.C. § 830 (regulation of listed
5 chemicals and certain machines);

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

9 (13) information that originates from, or is intermingled so as to be
10 indistinguishable from, information described in subdivision (12) of this
11 subsection and that a controller or processor collects, processes, uses, or
12 maintains in the same manner as is required under the law and regulations
13 specified in subdivision (12) of this subsection;

14 (14) a financial institution, credit union, independent trust company,
15 broker-dealer, or investment adviser or a financial institution's, credit union's,
16 independent trust company's, broker-dealer's, or investment adviser's affiliate
17 or subsidiary that is only and directly engaged in financial activities, as
18 described in 12 U.S.C. § 1843(k);

19 (15) a person regulated pursuant to part 3 of Title 8 (chapters 101–165)
20 other than a person that, alone or in combination with another person,

1 establishes and maintains a self-insurance program and that does not otherwise
2 engage in the business of entering into policies of insurance;

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

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

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

11 (19) noncommercial activity of:

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

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

17 (C) a nonprofit organization that provides programming to radio or
18 television networks; or

19 (D) an entity that provides an information service, including a press
20 association or wire service.

1 (b) Controllers, processors, and consumer health data controllers that
2 comply with the verifiable parental consent requirements of COPPA shall be
3 deemed compliant with any obligation to obtain parental consent pursuant to
4 this chapter, including pursuant to section 2420 of this title.

5 § 2418. CONSUMER PERSONAL DATA RIGHTS

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

7 (1) confirm whether or not a controller is processing the consumer’s
8 personal data and access the personal data, unless the confirmation or access
9 would require the controller to reveal a trade secret;

10 (2) obtain from a controller a list of third parties, other than individuals,
11 to which the controller has transferred, at the controller’s election, either the
12 consumer’s personal data or any personal data;

13 (3) correct inaccuracies in the consumer’s personal data, taking into
14 account the nature of the personal data and the purposes of the processing of
15 the consumer’s personal data;

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

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

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

2 (A) targeted advertising;

3 (B) the sale of personal data; or

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

6 (b)(1) A consumer may exercise rights under this section by submitting a
7 request to a controller using the method that the controller specifies in the
8 privacy notice under section 2419 of this title.

9 (2) A controller shall not require a consumer to create an account for the
10 purpose described in subdivision (1) of this subsection, but the controller may
11 require the consumer to use an account the consumer previously created.

12 (3) A parent or legal guardian may exercise rights under this section on
13 behalf of the parent’s child or on behalf of a child for whom the guardian has
14 legal responsibility. A guardian or conservator may exercise the rights under
15 this section on behalf of a consumer that is subject to a guardianship,
16 conservatorship, or other protective arrangement.

17 (4)(A) A consumer may designate another person to act on the
18 consumer’s behalf as the consumer’s authorized agent for the purpose of
19 exercising the consumer’s rights under subdivision (a)(4) or (a)(6) of this
20 section.

1 (B) The consumer may designate an authorized agent by means of an
2 internet link, browser setting, browser extension, global device setting, or other
3 technology that enables the consumer to exercise the consumer’s rights under
4 subdivision (a)(4) or (a)(6) of this section.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16 (A) the use of any false, fictitious, fraudulent, or materially
17 misleading statement or representation; or

18 (B) the employment of any dark pattern.

19 (d) A controller shall establish a process by means of which a consumer
20 may appeal the controller’s refusal to take action on a request under
21 subsection (b) of this section. The controller’s process must:

1 (1) Allow a reasonable period of time after the consumer receives the
2 controller’s refusal within which to appeal.

3 (2) Be conspicuously available to the consumer.

4 (3) Be similar to the manner in which a consumer must submit a request
5 under subsection (b) of this section.

6 (4) Require the controller to approve or deny the appeal within 45 days
7 after the date on which the controller received the appeal and to notify the
8 consumer in writing of the controller’s decision and the reasons for the
9 decision. If the controller denies the appeal, the notice must provide or specify
10 information that enables the consumer to contact the Attorney General to
11 submit a complaint.

12 § 2419. DUTIES OF CONTROLLERS

13 (a) A controller shall:

14 (1) specify in the privacy notice described in subsection (d) of this
15 section the express purposes for which the controller is collecting and
16 processing personal data;

17 (2) process personal data only:

18 (A) as reasonably necessary and proportionate to provide the services
19 for which the personal data was collected, consistent with the reasonable
20 expectations of the consumer whose personal data is being processed;

1 (B) for another disclosed purpose that is compatible with the context
2 in which the personal data was collected; or

3 (C) for a further disclosed purpose if the controller obtains the
4 consumer’s consent;

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

9 (4) provide an effective mechanism for a consumer to revoke consent to
10 the controller’s processing of the consumer’s personal data that is at least as
11 easy as the mechanism by which the consumer provided the consumer’s
12 consent and, upon revocation of the consent, cease to process the data as soon
13 as practicable, but not later than 15 days after receiving the request.

14 (b) A controller shall not:

15 (1) process personal data beyond what is reasonably necessary and
16 proportionate to the processing purpose;

17 (2) process sensitive data about a consumer without first obtaining the
18 consumer’s consent or, if the controller knows the consumer is a child, without
19 processing the sensitive data in accordance with COPPA;

20 (3)(A) except as provided in subdivision (B) of this subdivision (3),
21 process a consumer’s personal data in a manner that discriminates against

1 individuals or otherwise makes unavailable the equal enjoyment of goods or
2 services on the basis of an individual’s actual or perceived race, color, sex,
3 sexual orientation or gender identity, physical or mental disability, religion,
4 ancestry, or national origin;

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

6 (i) a private establishment, as that term is used in 42 U.S.C.
7 § 2000a(e) (prohibition against discrimination or segregation in places of
8 public accommodation);

9 (ii) processing for the purpose of a controller’s or processor’s self-
10 testing to prevent or mitigate unlawful discrimination; or

11 (iii) processing for the purpose of diversifying an applicant,
12 participant, or consumer pool.

13 (4) process a consumer’s personal data for the purposes of targeted
14 advertising, of profiling the consumer in furtherance of decisions that produce
15 legal or similarly significant effects concerning the consumer, or of selling the
16 consumer’s personal data without the consumer’s consent if the controller has
17 actual knowledge that, or willfully disregards whether, the consumer is at least
18 13 years of age and not older than 16 years of age; or

19 (5) discriminate or retaliate against a consumer who exercises a right
20 provided to the consumer under this chapter or refuses to consent to the

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

2 including by:

3 (A) denying goods or services;

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

5 (C) providing a different level of quality or selection of goods or
6 services to the consumer.

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

8 (1) require a controller to provide a good or service that requires
9 personal data from a consumer that the controller does not collect or maintain;

10 or

11 (2) prohibit a controller from offering a different price, rate, level of
12 quality, or selection of goods or services to a consumer, including an offer for
13 no fee or charge, in connection with a consumer's voluntary participation in a
14 financial incentive program, such as a bona fide loyalty, rewards, premium
15 features, discount, or club card program, provided that the controller may not
16 transfer personal data to a third party as part of the program unless:

17 (A) the transfer is necessary to enable the third party to provide a
18 benefit to which the consumer is entitled; or

19 (B)(i) the terms of the program clearly disclose that personal data
20 will be transferred to the third party or to a category of third parties of which
21 the third party belongs; and

1 (ii) the consumer consents to the transfer.

2 (d)(1) A controller shall provide to consumers a reasonably accessible,
3 clear, and meaningful privacy notice that:

4 (A) lists the categories of personal data, including the categories of
5 sensitive data, that the controller processes;

6 (B) describes the controller’s purposes for processing the personal
7 data;

8 (C) describes how a consumer may exercise the consumer’s rights
9 under this chapter, including how a consumer may appeal a controller’s denial
10 of a consumer’s request under section 2418 of this title;

11 (D) lists all categories of personal data, including the categories of
12 sensitive data, that the controller shares with third parties;

13 (E) describes all categories of third parties with which the controller
14 shares personal data at a level of detail that enables the consumer to understand
15 what type of entity each third party is and, to the extent possible, how each
16 third party may process personal data;

17 (F) specifies an e-mail address or other online method by which a
18 consumer can contact the controller that the controller actively monitors;

19 (G) identifies the controller, including any business name under
20 which the controller registered with the Secretary of State and any assumed
21 business name that the controller uses in this State;

1 (H) provides a clear and conspicuous description of any processing of
2 personal data in which the controller engages for the purposes of targeted
3 advertising, sale of personal data to third parties, or profiling the consumer in
4 furtherance of decisions that produce legal or similarly significant effects
5 concerning the consumer, and a procedure by which the consumer may opt out
6 of this type of processing; and

7 (I) describes the method or methods the controller has established for
8 a consumer to submit a request under subdivision 2418(b)(1) of this title.

9 (2) The privacy notice shall adhere to the accessibility and usability
10 guidelines recommended under 42 U.S.C. chapter 126 (the Americans with
11 Disabilities Act) and 29 U.S.C. 794d (section 508 of the Rehabilitation Act of
12 1973), including ensuring readability for individuals with disabilities across
13 various screen resolutions and devices and employing design practices that
14 facilitate easy comprehension and navigation for all users.

15 (e) The method or methods under subdivision (d)(1)(I) of this section for
16 submitting a consumer’s request to a controller must:

17 (1) take into account the ways in which consumers normally interact
18 with the controller, the need for security and reliability in communications
19 related to the request, and the controller’s ability to authenticate the identity of
20 the consumer that makes the request;

1 (2) provide a clear and conspicuous link to a website where the
2 consumer or an authorized agent may opt out from a controller’s processing of
3 the consumer’s personal data pursuant to subdivision 2418(a)(6) of this title or,
4 solely if the controller does not have a capacity needed for linking to a
5 webpage, provide another method the consumer can use to opt out; and

6 (3) allow a consumer or authorized agent to send a signal to the
7 controller that indicates the consumer’s preference to opt out of the sale of
8 personal data or targeted advertising pursuant to subdivision 2418(a)(6) of this
9 title by means of a platform, technology, or mechanism that:

10 (A) does not unfairly disadvantage another controller;

11 (B) does not use a default setting but instead requires the consumer or
12 authorized agent to make an affirmative, voluntary, and unambiguous choice to
13 opt out;

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

15 (D) is as consistent as possible with similar platforms, technologies,
16 or mechanisms required under federal or state laws or regulations; and

17 (E) enables the controller to reasonably determine whether the
18 consumer has made a legitimate request pursuant to subsection 2418(b) of this
19 title to opt out pursuant to subdivision 2418(a)(6) of this title.

20 (f) If a consumer or authorized agent uses a method under subdivision
21 (d)(1)(I) of this section to opt out of a controller’s processing of the

1 consumer’s personal data pursuant to subdivision 2418(a)(6) of this title and
2 the decision conflicts with a consumer’s voluntary participation in a bona fide
3 reward, club card, or loyalty program or a program that provides premium
4 features or discounts in return for the consumer’s consent to the controller’s
5 processing of the consumer’s personal data, the controller may either comply
6 with the request to opt out or notify the consumer of the conflict and ask the
7 consumer to affirm that the consumer intends to withdraw from the bona fide
8 reward, club card, or loyalty program or the program that provides premium
9 features or discounts. If the consumer affirms that the consumer intends to
10 withdraw, the controller shall comply with the request to opt out.

11 § 2420. DUTIES OF CONTROLLERS TO MINORS

12 (a)(1) A controller that offers any online service, product, or feature to a
13 consumer whom the controller actually knows or willfully disregards is a
14 minor shall use reasonable care to avoid any heightened risk of harm to minors
15 caused by the online service, product, or feature.

16 (2) In any action brought pursuant to section 2427, there is a rebuttable
17 presumption that a controller used reasonable care as required under this
18 section if the controller complied with this section.

19 (b) Unless a controller has obtained consent in accordance with subsection
20 (c) of this section, a controller that offers any online service, product, or

1 feature to a consumer whom the controller actually knows or willfully
2 disregards is a minor shall not:

3 (1) process a minor’s personal data for the purposes of:

4 (A) targeted advertising;

5 (B) the sale of personal data; or

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

8 (2) process a minor’s personal data for any purpose other than:

9 (A) the processing purpose that the controller disclosed at the time
10 the controller collected the minor’s personal data; or

11 (B) a processing purpose that is reasonably necessary for, and
12 compatible with, the processing purpose that the controller disclosed at the
13 time the controller collected the minor’s personal data; or

14 (3) process a minor’s personal data for longer than is reasonably
15 necessary to provide the online service, product, or feature;

16 (4) use any system design feature, except for a service or application that
17 is used by and under the direction of an educational entity, to significantly
18 increase, sustain, or extend a minor’s use of the online service, product, or
19 feature; or

20 (5) collect a minor’s precise geolocation data unless:

1 (A) the minor’s precise geolocation data is reasonably necessary for
2 the controller to provide the online service, product, or feature;

3 (B) the controller only collects the minor’s precise geolocation data
4 for the time necessary to provide the online service, product, or feature; and

5 (C) the controller provides to the minor a signal indicating that the
6 controller is collecting the minor’s precise geolocation data and makes the
7 signal available to the minor for the entire duration of the collection of the
8 minor’s precise geolocation data.

9 (c) A controller shall not engage in the activities described in subsection (b)
10 of this section unless the controller obtains:

11 (1) the minor’s consent; or

12 (2) if the minor is a child, the consent of the minor’s parent or legal
13 guardian.

14 (d) A controller that offers any online service, product, or feature to a
15 consumer whom that controller actually knows or willfully disregards is a
16 minor shall not:

17 (1) employ any dark pattern; or

18 (2) except as provided in subsection (e) of this section, offer any direct
19 messaging apparatus for use by a minor without providing readily accessible
20 and easy-to-use safeguards to limit the ability of an adult to send unsolicited
21 communications to the minor with whom the adult is not connected.

1 (e) Subdivision (d)(2) of this section does not apply to an online service,
2 product, or feature of which the predominant or exclusive function is:

3 (1) e-mail; or

4 (2) direct messaging consisting of text, photographs, or videos that are
5 sent between devices by electronic means, where messages are:

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

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

8 (C) not posted publicly.

9 § 2421. DUTIES OF PROCESSORS

10 (a) A processor shall adhere to a controller’s instructions and shall assist
11 the controller in meeting the controller’s obligations under this chapter. In
12 assisting the controller, the processor must:

13 (1) enable the controller to respond to requests from consumers pursuant
14 to subsection 2418(b) of this title by means that:

15 (A) take into account how the processor processes personal data and
16 the information available to the processor; and

17 (B) use appropriate technical and organizational measures to the
18 extent reasonably practicable;

19 (2) adopt administrative, technical, and physical safeguards that are
20 reasonably designed to protect the security and confidentiality of the personal

1 data the processor processes, taking into account how the processor processes
2 the personal data and the information available to the processor; and

3 (3) provide information reasonably necessary for the controller to
4 conduct and document data protection assessments.

5 (b) Processing by a processor must be governed by a contract between the
6 controller and the processor. The contract must:

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

8 (2) set forth clear instructions for processing data, the nature and
9 purpose of the processing, the type of data that is subject to processing, and the
10 duration of the processing;

11 (3) specify the rights and obligations of both parties with respect to the
12 subject matter of the contract;

13 (4) ensure that each person that processes personal data is subject to a
14 duty of confidentiality with respect to the personal data;

15 (5) require the processor to delete the personal data or return the
16 personal data to the controller at the controller’s direction or at the end of the
17 provision of services, unless a law requires the processor to retain the personal
18 data;

19 (6) require the processor to make available to the controller, at the
20 controller’s request, all information the controller needs to verify that the

1 processor has complied with all obligations the processor has under this
2 chapter;

3 (7) require the processor to enter into a subcontract with a person the
4 processor engages to assist with processing personal data on the controller’s
5 behalf and in the subcontract require the subcontractor to meet the processor’s
6 obligations concerning personal data;

7 (8)(A) allow the controller, the controller’s designee, or a qualified and
8 independent person the processor engages, in accordance with an appropriate
9 and accepted control standard, framework, or procedure, to assess the
10 processor’s policies and technical and organizational measures for complying
11 with the processor’s obligations under this chapter;

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

13 (C) at the controller’s request, report the results of the assessment to
14 the controller; and

15 (9) prohibit the processor from combining personal data obtained from
16 the controller with personal data that the processor:

17 (A) receives from or on behalf of another controller or person; or

18 (B) collects from an individual.

19 (c) This section does not relieve a controller or processor from any liability
20 that accrues under this chapter as a result of the controller’s or processor’s
21 actions in processing personal data.

1 (d)(1) For purposes of determining obligations under this chapter, a person
2 is a controller with respect to processing a set of personal data and is subject to
3 an action under section 2427 of this title to punish a violation of this chapter, if
4 the person:

5 (A) does not adhere to a controller’s instructions to process the
6 personal data; or

7 (B) begins at any point to determine the purposes and means for
8 processing the personal data, alone or in concert with another person.

9 (2) A determination under this subsection is a fact-based determination
10 that must take account of the context in which a set of personal data is
11 processed.

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

14 § 2422. DUTIES OF PROCESSORS TO MINORS

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

16 (1) assist the controller in meeting the controller’s obligations under
17 sections 2420 and 2424 of this title, taking into account:

18 (A) the nature of the processing;

19 (B) the information available to the processor by appropriate
20 technical and organizational measures; and

1 (C) whether the assistance is reasonably practicable and necessary to
2 assist the controller in meeting its obligations; and

3 (2) provide any information that is necessary to enable the controller to
4 conduct and document data protection assessments pursuant to section 2424 of
5 this title.

6 (b) A contract between a controller and a processor must satisfy the
7 requirements in subsection 2421(b) of this title.

8 (c) Nothing in this section shall be construed to relieve a controller or
9 processor from the liabilities imposed on the controller or processor by virtue
10 of the controller’s or processor’s role in the processing relationship as
11 described in sections 2420 and 2424 of this title.

12 (d) Determining whether a person is acting as a controller or processor with
13 respect to a specific processing of data is a fact-based determination that
14 depends upon the context in which personal data is to be processed. A person
15 that is not limited in the person’s processing of personal data pursuant to a
16 controller’s instructions, or that fails to adhere to the instructions, is a
17 controller and not a processor with respect to a specific processing of data. A
18 processor that continues to adhere to a controller’s instructions with respect to
19 a specific processing of personal data remains a processor. If a processor
20 begins, alone or jointly with others, determining the purposes and means of the
21 processing of personal data, the processor is a controller with respect to the

1 processing and may be subject to an enforcement action under section 2427 of
2 this title.

3 § 2423. DATA PROTECTION ASSESSMENTS FOR PROCESSING

4 ACTIVITIES THAT PRESENT A HEIGHTENED RISK OF HARM
5 TO A CONSUMER

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

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

11 (2) the sale of personal data;

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

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

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

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

20 (D) other substantial injury to consumers; and

21 (4) the processing of sensitive data.

1 (b)(1) Data protection assessments conducted pursuant to subsection (a) of
2 this section shall:

3 (A) identify the categories of personal data processed, the purposes
4 for processing the personal data, and whether the personal data is being
5 transferred to third parties; and

6 (B) identify and weigh the benefits that may flow, directly and
7 indirectly, from the processing to the controller, the consumer, other
8 stakeholders, and the public against the potential risks to the consumer
9 associated with the processing, as mitigated by safeguards that can be
10 employed by the controller to reduce the risks.

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

15 (c)(1) The Attorney General may require that a controller disclose any data
16 protection assessment that is relevant to an investigation conducted by the
17 Attorney General pursuant to section 2427 of this title, and the controller shall
18 make the data protection assessment available to the Attorney General.

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

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

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

7 (d) A single data protection assessment may address a comparable set of
8 processing operations that present a similar heightened risk of harm.

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

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

17 (g) A controller shall retain for at least five years all data protection
18 assessments the controller conducts under this section.

1 § 2424. DATA PROTECTION ASSESSMENTS FOR ONLINE SERVICES,
2 PRODUCTS, OR FEATURES OFFERED TO MINORS

3 (a) A controller that offers any online service, product, or feature to a
4 consumer whom the controller actually knows or willfully disregards is a
5 minor shall conduct a data protection assessment for the online service product
6 or feature:

7 (1) in a manner that is consistent with the requirements established in
8 section 2423 of this title; and

9 (2) that addresses:

10 (A) the purpose of the online service, product, or feature;

11 (B) the categories of a minor’s personal data that the online service,
12 product, or feature processes;

13 (C) the purposes for which the controller processes a minor’s
14 personal data with respect to the online service, product, or feature; and

15 (D) any heightened risk of harm to a minor that is a reasonably
16 foreseeable result of offering the online service, product, or feature to a minor.

17 (b) A controller that conducts a data protection assessment pursuant to
18 subsection (a) of this section shall review the data protection assessment as
19 necessary to account for any material change to the processing operations of
20 the online service, product, or feature that is the subject of the data protection
21 assessment.

1 (c) If a controller conducts a data protection assessment pursuant to
2 subsection (a) of this section or a data protection assessment review pursuant
3 to subsection (b) of this section and determines that the online service, product,
4 or feature that is the subject of the assessment poses a heightened risk of harm
5 to a minor, the controller shall establish and implement a plan to mitigate or
6 eliminate the heightened risk.

7 (d)(1) The Attorney General may require that a controller disclose any data
8 protection assessment pursuant to subsection (a) of this section that is relevant
9 to an investigation conducted by the Attorney General pursuant to section 2427
10 of this title, and the controller shall make the data protection assessment
11 available to the Attorney General.

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

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

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

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

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

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

9 (h) A controller that conducts a data protection assessment pursuant to
10 subsection (a) of this section shall maintain documentation concerning the data
11 protection assessment for the longer of:

12 (1) three years after the date on which the processing operations cease;

13 or

14 (2) the date the controller ceases offering the online service, product, or
15 feature.

16 § 2425. DE-IDENTIFIED OR PSEUDONYMOUS DATA

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

18 (1) follow industry best-practices to ensure that the data cannot be used
19 to re-identify an identified or identifiable individual or be associated with an
20 individual or device that identifies or is linked or reasonably linkable to an
21 individual or household;

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

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

5 (b) This section does not prohibit a controller from attempting to re-
6 identify de-identified data solely for the purpose of testing the controller’s
7 methods for de-identifying data.

8 (c) This chapter shall not be construed to require a controller or processor
9 to:

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

11 (2) maintain data in identifiable form, or collect, obtain, retain, or access
12 any data or technology, in order to associate a consumer with personal data in
13 order to authenticate the consumer’s request under subsection 2418(b) of this
14 title; or

15 (3) comply with an authenticated consumer rights request if the
16 controller:

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

1 (B) does not use the personal data to recognize or respond to the
2 specific consumer who is the subject of the personal data or associate the
3 personal data with other personal data about the same specific consumer; and

4 (C) does not sell or otherwise voluntarily disclose the personal data
5 to any third party, except as otherwise permitted in this section.

6 (d) The rights afforded under subdivisions 2418(a)(1)–(5) of this title shall
7 not apply to pseudonymous data in cases where the controller is able to
8 demonstrate that any information necessary to identify the consumer is kept
9 separately and is subject to effective technical and organizational controls that
10 prevent the controller from accessing the information.

11 (e) A controller that discloses or transfers pseudonymous data or de-
12 identified data shall exercise reasonable oversight to monitor compliance with
13 any contractual commitments to which the pseudonymous data or de-identified
14 data is subject and shall take appropriate steps to address any breaches of those
15 contractual commitments.

16 § 2426. CONSTRUCTION OF DUTIES OF CONTROLLERS AND
17 PROCESSORS

18 (a) This chapter shall not be construed to restrict a controller’s, processor’s,
19 or consumer health data controller’s ability to:

20 (1) comply with federal, state, or municipal laws, ordinances, or
21 regulations;

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

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

8 (4) carry out obligations under a contract under subsection 2421(b) of
9 this title for a federal or State agency or local unit of government;

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

11 (6) provide a product or service specifically requested by the consumer
12 to whom the personal data pertains;

13 (7) perform under a contract to which a consumer is a party, including
14 fulfilling the terms of a written warranty;

15 (8) take steps at the request of a consumer prior to entering into a
16 contract;

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

1 (10) prevent, detect, protect against, or respond to a network security or
2 physical security incident, including an intrusion or trespass, medical alert, or
3 fire alarm;

4 (11) prevent, detect, protect against, or respond to identity theft, fraud,
5 harassment, malicious or deceptive activity, or any criminal activity targeted at
6 or involving the controller or processor or its services, preserve the integrity or
7 security of systems, or investigate, report, or prosecute those responsible for
8 the action;

9 (12) assist another controller, processor, consumer health data
10 controller, or third party with any of the obligations under this chapter; or

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

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

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

18 (b) The obligations imposed on controllers, processors, or consumer health
19 data controllers under this chapter shall not restrict a controller's, processor's,
20 or consumer health data controller's ability to collect, use, or retain data for
21 internal use to:

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

3 (2) effectuate a product recall; or

4 (3) identify and repair technical errors that impair existing or intended
5 functionality.

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

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

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

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

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

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

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

12 (B) under 12 V.S.A. § 1615; or

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

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

18 (A)(i) reasonably necessary and proportionate to the purposes listed
19 in this section; or

20 (ii) in the case of sensitive data, strictly necessary to the purposes
21 listed in this section; and

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

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

6 (B) Personal data collected, used, or retained pursuant to subsection
7 (b) of this section shall be subject to reasonable administrative, technical, and
8 physical measures to protect the confidentiality, integrity, and accessibility of
9 the personal data and to reduce reasonably foreseeable risks of harm to
10 consumers relating to the collection, use, or retention of personal data.

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

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

1 § 2427. ENFORCEMENT: PRIVATE RIGHT OF ACTION AND
2 ATTORNEY GENERAL’S POWERS

3 (a)(1) A person who violates this chapter or rules adopted pursuant to this
4 chapter commits an unfair and deceptive act in commerce in violation of
5 section 2453 of this title.

6 (2) A consumer harmed by a violation of this chapter or rules adopted
7 pursuant to this chapter may bring an action in Superior Court for the greater
8 of \$1,000.00 or actual damages, injunctive relief, punitive damages in the case
9 of an intentional violation, and reasonable costs and attorney’s fees if the
10 consumer has notified the controller or processor of the violation and the
11 controller or processor fails to cure the violation within 60 days following
12 receipt of the notice of violation.

13 (b)(1) The Attorney General may, prior to initiating any action for a
14 violation of any provision of this chapter, issue a notice of violation to the
15 controller or consumer health data controller if the Attorney General
16 determines that a cure is possible.

17 (2) The Attorney General may, in determining whether to grant a
18 controller, processor, or consumer health data controller the opportunity to
19 cure an alleged violation described in subdivision (1) of this subsection,
20 consider:

21 (A) the number of violations;

1 (B) the size and complexity of the controller, processor, or consumer
2 health data controller;

3 (C) the nature and extent of the controller’s, processor’s, or consumer
4 health data controller’s processing activities;

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

6 (E) the safety of persons or property;

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

9 (G) the sensitivity of the data.

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

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

13 (2) the nature of each violation;

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

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

18 § 2428. CONFIDENTIALITY OF CONSUMER HEALTH DATA

19 Except as provided in subsections 2417(a) and (b) of this title and section
20 2426 of this title, no person shall:

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

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

6 (3) use a geofence to establish a virtual boundary that is within 1,850
7 feet of any health care facility, mental health facility, or reproductive or sexual
8 health facility for the purpose of identifying, tracking, collecting data from, or
9 sending any notification to a consumer regarding the consumer’s consumer
10 health data; or

11 (4) sell or offer to sell consumer health data without first obtaining the
12 consumer’s consent.

13 Sec. 2. PUBLIC EDUCATION AND OUTREACH; ATTORNEY GENERAL
14 STUDY

15 (a) The Attorney General and the Agency of Commerce and Community
16 Development shall implement a comprehensive public education, outreach,
17 and assistance program for controllers and processors, as those terms are
18 defined in 9 V.S.A. § 2415. The program shall focus on:

19 (1) the requirements and obligations of controllers and processors under
20 the Vermont Data Privacy Act;

21 (2) data protection assessments under 9 V.S.A. § 2421;

1 (3) enhanced protections that apply to children, minors, sensitive data,
2 or consumer health data, as those terms are defined in 9 V.S.A. § 2415;

3 (4) a controller’s obligations to law enforcement agencies and the
4 Attorney General’s office;

5 (5) methods for conducting data inventories; and

6 (6) any other matters the Attorney General or the Agency of Commerce
7 and Community Development deems appropriate.

8 (b) The Attorney General and the Agency of Commerce and Community
9 Development shall provide guidance to controllers for establishing data
10 privacy notices and opt-out mechanisms, which may be in the form of
11 templates.

12 (c) The Attorney General and the Agency of Commerce and Community
13 Development shall implement a comprehensive public education, outreach,
14 and assistance program for consumers, as that term is defined in 9 V.S.A.
15 § 2415. The program shall focus on:

16 (1) the rights afforded consumers under the Vermont Data Privacy Act,
17 including:

18 (A) the methods available for exercising data privacy rights; and

19 (B) the opt-out mechanism available to consumers;

20 (2) the obligations controllers have to consumers;

1 (3) different treatment of children, minors, and other consumers under
2 the act, including the different consent mechanisms in place for children and
3 other consumers;

4 (4) understanding a privacy notice provided under the act;

5 (5) the different enforcement mechanisms available under the act,
6 including the consumer’s private right of action; and

7 (6) any other matters the Attorney General or the Agency of Commerce
8 and Community Development deems appropriate.

9 (d) The Attorney General and the Agency of Commerce and Community
10 Development shall cooperate with states with comparable data privacy regimes
11 to develop any outreach, assistance, and education programs, where
12 appropriate.

13 (e) On or before December 15, 2026, the Attorney General shall assess the
14 effectiveness of the implementation of the act and submit a report to the House
15 Committee on Commerce and Economic Development and the Senate
16 Committee on Economic Development, Housing and General Affairs with its
17 findings and recommendations, including any proposed draft legislation to
18 address issues that have arisen since implementation.

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

2 CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

3 Subchapter 1. General Provisions

4 § 2430. DEFINITIONS

5 As used in this chapter:

6 (1) “Biometric data” shall have the same meaning as in section 2415 of
7 this title.

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

11 (i) name;

12 (ii) address;

13 (iii) date of birth;

14 (iv) place of birth;

15 (v) mother’s maiden name;

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

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

3 (viii) Social Security number or other government-issued
4 identification number; or

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

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

11 ~~(2)~~(3) “Business” means a controller, a consumer health data controller ,
12 or a commercial entity, including a sole proprietorship, partnership,
13 corporation, association, limited liability company, or other group, however
14 organized and whether or not organized to operate at a profit, including a
15 financial institution organized, chartered, or holding a license or authorization
16 certificate under the laws of this State, any other state, the United States, or any
17 other country, or the parent, affiliate, or subsidiary of a financial institution,
18 but does not include the State, a State agency, any political subdivision of the
19 State, or a vendor acting solely on behalf of, and at the direction of, the State.

1 ~~(3)~~(4) “Consumer” means an individual ~~residing in this State~~ who is a
2 resident of the State or an individual who is in the State at the time a data
3 broker collects the individual’s data.

4 (5) “Consumer health data controller” has the same meaning as in
5 section 2415 of this title.

6 (6) “Controller” has the same meaning as in section 2415 of this title.

7 ~~(4)~~(7)(A) “Data broker” means a business, or unit or units of a business,
8 separately or together, that knowingly collects and sells or licenses to third
9 parties the brokered personal information of a consumer with whom the
10 business does not have a direct relationship.

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

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

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

16 (iii) investor in the business; or

17 (iv) donor to the business.

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

1 (i) developing or maintaining third-party e-commerce or
2 application platforms;

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

6 (iii) providing publicly available information related to a
7 consumer’s business or profession; or

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

10 (D) The phrase “sells or licenses” does not include:

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

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

16 ~~(5)(8)~~(A) “Data broker security breach” means an unauthorized
17 acquisition or a reasonable belief of an unauthorized acquisition of more than
18 one element of brokered personal information maintained by a data broker
19 when the brokered personal information is not encrypted, redacted, or
20 protected by another method that renders the information unreadable or
21 unusable by an unauthorized person.

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

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

10 (i) indications that the brokered personal information is in the
11 physical possession and control of a person without valid authorization, such
12 as a lost or stolen computer or other device containing brokered personal
13 information;

14 (ii) indications that the brokered personal information has been
15 downloaded or copied;

16 (iii) indications that the brokered personal information was used
17 by an unauthorized person, such as fraudulent accounts opened or instances of
18 identity theft reported; or

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

20 ~~(6)(9)~~ “Data collector” means a person who, for any purpose, whether
21 by automated collection or otherwise, handles, collects, disseminates, or

1 otherwise deals with personally identifiable information, and includes the
2 State, State agencies, political subdivisions of the State, public and private
3 universities, privately and publicly held corporations, limited liability
4 companies, financial institutions, and retail operators.

5 ~~(7)~~(10) “Encryption” means use of an algorithmic process to transform
6 data into a form in which the data is rendered unreadable or unusable without
7 use of a confidential process or key.

8 ~~(8)~~(11) “License” means a grant of access to, or distribution of, data by
9 one person to another in exchange for consideration. A use of data for the sole
10 benefit of the data provider, where the data provider maintains control over the
11 use of the data, is not a license.

12 ~~(9)~~(12) “Login credentials” means a consumer’s user name or e-mail
13 address, in combination with a password or an answer to a security question,
14 that together permit access to an online account.

15 ~~(10)~~(13)(A) “Personally identifiable information” means a consumer’s
16 first name or first initial and last name in combination with one or more of the
17 following digital data elements, when the data elements are not encrypted,
18 redacted, or protected by another method that renders them unreadable or
19 unusable by unauthorized persons:

20 (i) a Social Security number;

1 (ii) a driver license or nondriver State identification card number,
2 individual taxpayer identification number, passport number, military
3 identification card number, or other identification number that originates from
4 a government identification document that is commonly used to verify identity
5 for a commercial transaction;

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

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

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

16 (vi) genetic information; and

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

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

21 (III) a health insurance policy number.

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

4 ~~(11)~~(14) “Record” means any material on which written, drawn, spoken,
5 visual, or electromagnetic information is recorded or preserved, regardless of
6 physical form or characteristics.

7 ~~(12)~~(15) “Redaction” means the rendering of data so that the data are
8 unreadable or are truncated so that ~~no~~ not more than the last four digits of the
9 identification number are accessible as part of the data.

10 ~~(13)~~(16)(A) “Security breach” means unauthorized acquisition of
11 electronic data, or a reasonable belief of an unauthorized acquisition of
12 electronic data, that compromises the security, confidentiality, or integrity of a
13 consumer’s personally identifiable information or login credentials maintained
14 by a data collector.

15 (B) “Security breach” does not include good faith but unauthorized
16 acquisition of personally identifiable information or login credentials by an
17 employee or agent of the data collector for a legitimate purpose of the data
18 collector, provided that the personally identifiable information or login
19 credentials are not used for a purpose unrelated to the data collector’s business
20 or subject to further unauthorized disclosure.

1 (C) In determining whether personally identifiable information or
2 login credentials have been acquired or is reasonably believed to have been
3 acquired by a person without valid authorization, a data collector may consider
4 the following factors, among others:

5 (i) indications that the information is in the physical possession
6 and control of a person without valid authorization, such as a lost or stolen
7 computer or other device containing information;

8 (ii) indications that the information has been downloaded or
9 copied;

10 (iii) indications that the information was used by an unauthorized
11 person, such as fraudulent accounts opened or instances of identity theft
12 reported; or

13 (iv) that the information has been made public.

14 * * *

15 Subchapter 2. ~~Security Breach Notice Act~~ Data Security Breaches

16 * * *

17 § 2436. NOTICE OF DATA BROKER SECURITY BREACH

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

20 (b) Notice of breach.

1 (1) Except as otherwise provided in subsection (c) of this section, any
2 data broker shall notify the consumer that there has been a data broker security
3 breach following discovery or notification to the data broker of the breach.
4 Notice of the security breach shall be made in the most expedient time possible
5 and without unreasonable delay, but not later than 45 days after the discovery
6 or notification, consistent with the legitimate needs of the law enforcement
7 agency, as provided in subdivisions (3) and (4) of this subsection, or with any
8 measures necessary to determine the scope of the security breach and restore
9 the reasonable integrity, security, and confidentiality of the data system.

10 (2) A data broker shall provide notice of a breach to the Attorney
11 General as follows:

12 (A)(i) The data broker shall notify the Attorney General of the date of
13 the security breach and the date of discovery of the breach and shall provide a
14 preliminary description of the breach within 14 business days, consistent with
15 the legitimate needs of the law enforcement agency, as provided in
16 subdivisions (3) and (4) of this subsection (b), after the data broker’s discovery
17 of the security breach or when the data broker provides notice to consumers
18 pursuant to this section, whichever is sooner.

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

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

7 (B)(i) When the data broker provides notice of the breach pursuant to
8 subdivision (1) of this subsection (b), the data broker shall notify the Attorney
9 General of the number of Vermont consumers affected, if known to the data
10 broker, and shall provide a copy of the notice provided to consumers under
11 subdivision (1) of this subsection (b).

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

16 (3) The notice to a consumer required by this subsection shall be
17 delayed upon request of a law enforcement agency. A law enforcement agency
18 may request the delay if it believes that notification may impede a law
19 enforcement investigation or a national or Homeland Security investigation or
20 jeopardize public safety or national or Homeland Security interests. In the
21 event law enforcement makes the request for a delay in a manner other than in

1 writing, the data broker shall document the request contemporaneously in
2 writing and include the name of the law enforcement officer making the
3 request and the officer’s law enforcement agency engaged in the investigation.
4 A law enforcement agency shall promptly notify the data broker in writing
5 when the law enforcement agency no longer believes that notification may
6 impede a law enforcement investigation or a national or Homeland Security
7 investigation, or jeopardize public safety or national or Homeland Security
8 interests. The data broker shall provide notice required by this section without
9 unreasonable delay upon receipt of a written communication, which includes
10 facsimile or electronic communication, from the law enforcement agency
11 withdrawing its request for delay.

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

16 (A) the incident in general terms;

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

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

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

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

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

6 (5) A data broker may provide notice of a security breach involving
7 brokered personal information to a consumer by two or more of the following
8 methods:

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

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

12 (i) the data broker’s primary method of communication with the
13 consumer is by electronic means, the electronic notice does not request or
14 contain a hypertext link to a request that the consumer provide personal
15 information, and the electronic notice conspicuously warns consumers not to
16 provide personal information in response to electronic communications
17 regarding security breaches; or

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

1 (C) telephonic notice, provided that telephonic contact is made
2 directly with each affected consumer and not through a prerecorded message;
3 or

4 (D) notice by publication in a newspaper of statewide circulation in
5 the event the data broker cannot effectuate notice by any other means.

6 (c) Exception.

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

20 (2) If a data broker established that misuse of brokered personal
21 information was not reasonably possible under subdivision (1) of this

1 subsection and subsequently obtains facts indicating that misuse of the
2 brokered personal information has occurred or is occurring, the data broker
3 shall provide notice of the security breach pursuant to subsection (b) of this
4 section.

5 (d) Waiver. Any waiver of the provisions of this subchapter is contrary to
6 public policy and is void and unenforceable.

7 (e) Enforcement.

8 (1) With respect to a controller or processor other than a controller or
9 processor licensed or registered with the Department of Financial Regulation
10 under title 8 or this title, the Attorney General and State’s Attorney shall have
11 sole and full authority to investigate potential violations of this chapter and to
12 enforce, prosecute, obtain, and impose remedies for a violation of this chapter
13 or any rules or regulations adopted pursuant to this chapter as the Attorney
14 General and State’s Attorney have under chapter 63 of this title. The Attorney
15 General may refer the matter to the State’s Attorney in an appropriate case.
16 The Superior Courts shall have jurisdiction over any enforcement matter
17 brought by the Attorney General or a State’s Attorney under this subsection.

18 (2) With respect to a controller or processor that is licensed or registered
19 with the Department of Financial Regulation under title 8 or this title, the
20 Department of Financial Regulation shall have the full authority to investigate
21 potential violations of this chapter and to enforce, prosecute, obtain, and

1 impose remedies for a violation of this chapter or any rules or regulations
2 adopted pursuant to this chapter, as the Department has under title 8 or this title
3 or any other applicable law or regulation.

4 * * *

5 Subchapter 5. Data Brokers

6 § 2446. DATA BROKERS; ANNUAL REGISTRATION

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

10 (1) register with the Secretary of State;

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

12 (3) provide the following information:

13 (A) the name and primary physical, e-mail, and ~~Internet~~ internet
14 addresses of the data broker;

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

18 ~~(i) the method for requesting an opt out;~~

19 ~~(ii) if the opt out applies to only certain activities or sales, which~~
20 ~~ones; and~~

1 ~~(iii)~~ and whether the data broker permits a consumer to authorize a
2 third party to perform the opt-out on the consumer’s behalf;

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

5 ~~(D) a statement whether the data broker implements a purchaser~~
6 ~~credentialing process;~~

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

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

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

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

18 (1) a civil penalty of ~~\$50.00~~ \$125.00 for each day, ~~not to exceed a total~~
19 ~~of \$10,000.00 for each year,~~ it fails to register pursuant to this section;

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

1 (3) other penalties imposed by law.

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

6 (d) A data broker that files materially incorrect information in its
7 registration:

8 (1) is liable to the State for a civil penalty of \$25,000.00; and

9 (2) if it fails to correct the false information within five business days
10 after discovery or notification of the incorrect information, an additional civil
11 penalty of \$1,000.00 per day for each day thereafter that it fails to correct the
12 information.

13 (e) The Attorney General may maintain an action in the Civil Division of
14 the Superior Court to collect the penalties imposed in this section and to seek
15 appropriate injunctive relief.

16 * * *

17 § 2448. DATA BROKERS; ADDITIONAL DUTIES

18 (a) Individual opt-out.

19 (1) A consumer may request that a data broker do any of the following:

20 (A) stop collecting the consumer’s data;

21 (B) delete all data in its possession about the consumer; or

1 (C) stop selling the consumer’s data.

2 (2) Notwithstanding subsections 2418(c)–(d) of this title, a data broker
3 shall establish a simple procedure for consumers to submit a request and, shall
4 comply with a request from a consumer within 10 days after receiving the
5 request.

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

8 (b) General opt-out.

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

12 (2) On or before January 1, 2026, the Secretary of State shall develop an
13 online form to facilitate the general opt-out by a consumer and shall maintain a
14 Data Broker Opt-Out List of consumers who have requested a general opt-out,
15 with the specific type of opt-out.

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

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

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

3 (6) The Secretary of State shall implement and maintain reasonable
4 security procedures and practices to protect a consumer’s information under
5 the Data Broker Opt-Out List from unauthorized use, disclosure, access,
6 destruction, or modification, including administrative, physical, and technical
7 safeguards appropriate to the nature of the information and the purposes for
8 which the information will be used.

9 (7) The Secretary of State shall not charge a consumer to make an opt-
10 out request.

11 (8) The Data Broker Opt-Out List shall include an accessible deletion
12 mechanism that supports the ability of an authorized agent to act on behalf of a
13 consumer.

14 (c) Credentialing.

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

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

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

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

7 (d) Exemption. Nothing in this section applies to brokered personal
8 information that is:

9 (1) regulated as a consumer report pursuant to the Fair Credit Reporting
10 Act, 15 U.S.C. § 1681–1681x, if the data broker is fully complying with the
11 Act; or

12 (2) regulated pursuant to the Driver’s Privacy Protection Act of 1994,
13 18 U.S.C. § 2721–2725, if the data broker is fully complying with the Act.

14 Sec. 4. EFFECTIVE DATE

15 This act shall take effect on July 1, 2025.

16

17

18

19

20

21

1

2 (Committee vote: _____)

3

4

Representative _____

5

FOR THE COMMITTEE