

1 TO THE HOUSE OF REPRESENTATIVES:

2 The Committee on Commerce and Economic Development to which was  
3 referred Senate Bill No. 289 entitled “An act relating to age-appropriate design  
4 code” respectfully reports that it has considered the same and recommends that  
5 the House propose to the Senate that the bill be amended by striking out all  
6 after the enacting clause and inserting in lieu thereof the following:

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

8 CHAPTER 61A. VERMONT DATA PRIVACY ACT

9 § 2415. DEFINITIONS

10 As used in this chapter:

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

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

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

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

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

1           (2) “Age estimation” means a process that estimates that a consumer is  
2           likely to be of a certain age, fall within an age range, or is over or under a  
3           certain age.

4           (A) Age estimation methods include:

5           (i) analysis of behavioral and environmental data the controller  
6           already collects about its consumers;

7           (ii) comparing the way a consumer interacts with a device or with  
8           consumers of the same age;

9           (iii) metrics derived from motion analysis; and

10          (iv) testing a consumer’s capacity or knowledge.

11          (B) Age estimation does not require certainty, and if a controller  
12          estimates a consumer’s age for the purpose of advertising or marketing, that  
13          estimation may also be used to comply with this chapter.

14          (3) “Age verification” means a system that relies on hard identifiers or  
15          verified sources of identification to confirm a consumer has reached a certain  
16          age, including government-issued identification or a credit card.

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

1           (5)(A) “Biometric data” means data generated from the technological  
2           processing of an individual’s unique biological, physical, or physiological  
3           characteristics that is linked or reasonably linkable to an individual, including:

4                   (i) iris or retina scans;

5                   (ii) fingerprints;

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

7                   (iv) vein patterns;

8                   (v) voice prints; and

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

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

11                   (i) a digital or physical photograph;

12                   (ii) an audio or video recording; or

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

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

17           (7) “Business associate” has the same meaning as in HIPAA.

18           (8) “Child” has the same meaning as in COPPA.

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

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

3           (C) “Consent” does not include:

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

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

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

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

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

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

1           (12) “Consumer health data controller” means any controller that, alone  
2           or jointly with others, determines the purpose and means of processing  
3           consumer health data.

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

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

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

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

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

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

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

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

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

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

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

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

17 (C) contractually obligates any recipients of the data to satisfy the  
18 criteria set forth in subdivisions (A) and (B) of this subdivision (20).

19 (21) “Financial institution”:

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

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

3           (22) “Gender-affirming health care services” has the same meaning as in  
4           1 V.S.A. § 150.

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

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

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

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

14           (24) “Genetic data” means any data, regardless of its format, that results  
15           from the analysis of a biological sample of an individual, or from another  
16           source enabling equivalent information to be obtained, and concerns genetic  
17           material, including deoxyribonucleic acids (DNA), ribonucleic acids (RNA),  
18           genes, chromosomes, alleles, genomes, alterations or modifications to DNA or  
19           RNA, single nucleotide polymorphisms (SNPs), epigenetic markers,  
20           uninterpreted data that results from analysis of the biological sample or other  
21           source, and any information extrapolated, derived, or inferred therefrom.

1           (25) “Geofence” means any technology that uses global positioning  
2           coordinates, cell tower connectivity, cellular data, radio frequency  
3           identification, wireless fidelity technology data, or any other form of location  
4           detection, or any combination of such coordinates, connectivity, data,  
5           identification, or other form of location detection, to establish a virtual  
6           boundary.

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

8           (27) “Heightened risk of harm to a minor” means processing the  
9           personal data of a minor in a manner that presents a reasonably foreseeable risk  
10          of:

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

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

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

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

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



1           (29) “Identified or identifiable individual” means an individual who can  
2           be readily identified, directly or indirectly, including by reference to an  
3           identifier such as a name, an identification number, specific geolocation data,  
4           or an online identifier.

5           (30) “Independent trust company” has the same meaning as in 8 V.S.A.  
6           § 2401.

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

8           (32) “Mental health facility” means any health care facility in which at  
9           least 70 percent of the health care services provided in the facility are mental  
10           health services.

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

13           (34)(A) “Online service, product, or feature” means any service,  
14           product, or feature that is provided online, except as provided in subdivision  
15           (B) of this subdivision (34).

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

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

19           (ii) broadband internet access service, as that term is defined in  
20           47 C.F.R. § 54.400 (universal service support); or

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

1           (35) “Patient identifying information” has the same meaning as in  
2           42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

3           (36) “Patient safety work product” has the same meaning as in 42 C.F.R.  
4           § 3.20 (patient safety organizations and patient safety work product).

5           (37)(A) “Personal data” means any information, including derived data  
6           and unique identifiers, that is linked or reasonably linkable to an identified or  
7           identifiable individual or to a device that identifies, is linked to, or is  
8           reasonably linkable to one or more identified or identifiable individuals in a  
9           household.

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

12           (38)(A) “Precise geolocation data” means information derived from  
13           technology that can precisely and accurately identify the specific location of a  
14           consumer within a radius of 1,850 feet.

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

16                   (i) the content of communications;

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

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

20           (39) “Process” or “processing” means any operation or set of operations  
21           performed, whether by manual or automated means, on personal data or on sets

1 of personal data, such as the collection, use, storage, disclosure, analysis,  
2 deletion, or modification of personal data.

3 (40) “Processor” means a person who processes personal data on behalf  
4 of a controller.

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

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

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

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

16 (i) is lawfully made available through federal, state, or local  
17 government records; or

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

1           (B) “Publicly available information” does not include biometric data  
2           collected by a business about a consumer without the consumer’s knowledge.

3           (45) “Qualified service organization” has the same meaning as in  
4           42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

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

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

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

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

17           (B) As used in this subdivision (49), “commercial purpose” means to  
18           advance a person’s commercial or economic interests, such as by inducing  
19           another person to buy, rent, lease, join, subscribe to, provide, or exchange  
20           products, goods, property, information, or services, or enabling or effecting,  
21           directly or indirectly, a commercial transaction.

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

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

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

6                   (iii) the disclosure or transfer of personal data to an affiliate of the  
7 controller;

8                   (iv) the disclosure of personal data where the consumer directs the  
9 controller to disclose the personal data or intentionally uses the controller to  
10 interact with a third party;

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

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

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

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

19           (50) “Sensitive data” means personal data that:

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

4           (B) reveals a consumer’s racial or ethnic origin, national origin,  
5           citizenship or immigration status, religious or philosophical beliefs, or union  
6           membership;

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

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

10          (E) is financial information, including a consumer’s tax return and  
11          account number, financial account log-in, financial account, debit card number,  
12          or credit card number in combination with any required security or access  
13          code, password, or credentials allowing access to an account;

14          (F) is consumer health data;

15          (G) is personal data collected and analyzed concerning consumer  
16          health data or personal data that describes or reveals a past, present, or future  
17          mental or physical health condition, treatment, disability, or diagnosis,  
18          including pregnancy, to the extent the personal data is not used by the  
19          controller to identify a specific consumer’s physical or mental health condition  
20          or diagnosis;

21          (H) is biometric or genetic data;

1           (I) is personal data collected from a known minor; or

2           (J) is precise geolocation data.

3           (51)(A) “Targeted advertising” means the targeting of an advertisement  
4 to a consumer based on the consumer’s activity with one or more businesses,  
5 distinctly branded websites, applications, or services, other than the controller,  
6 distinctly branded website, application, or service with which the consumer is  
7 intentionally interacting.

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

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

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

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

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

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

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

1           (54) “Victim services organization” means a nonprofit organization that  
2           is established to provide services to victims or witnesses of child abuse,  
3           domestic violence, human trafficking, sexual assault, violent felony, or  
4           stalking.

5           § 2416. APPLICABILITY

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

10           (1) controlled or processed the personal data of not fewer than 25,000  
11           consumers, excluding personal data controlled or processed solely for the  
12           purpose of completing a payment transaction; or

13           (2) controlled or processed the personal data of not fewer than 12,500  
14           consumers and derived more than 25 percent of the person’s gross revenue  
15           from the sale of personal data.

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

20           § 2417. EXEMPTIONS

21           (a) This chapter does not apply to:



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

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

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

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

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

13           (B) research on human subjects undertaken in accordance with good  
14           clinical practice guidelines issued by the International Council for  
15           Harmonisation of Technical Requirements for Pharmaceuticals for Human  
16           Use;

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

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

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

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

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

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

20           (9) information processed or maintained solely in connection with, and  
21           for the purpose of, enabling;

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

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

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

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

7           (E) notice of an emergency to persons that an individual specifies;

8           (10) any activity that involves collecting, maintaining, disclosing,  
9 selling, communicating, or using information for the purpose of evaluating a  
10 consumer’s creditworthiness, credit standing, credit capacity, character,  
11 general reputation, personal characteristics, or mode of living if done strictly in  
12 accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C.  
13 § 1681–1681x, as may be amended, by:

14           (A) a consumer reporting agency;

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

18           (C) a person who uses a consumer report as provided in 15 U.S.C.  
19 § 1681b(a)(3) (permissible purposes of consumer reports);

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

1           (A) the Driver’s Privacy Protection Act of 1994, 18 U.S.C. § 2721–  
2           2725;

3           (B) the Family Educational Rights and Privacy Act, 20 U.S.C.  
4           § 1232g, and regulations adopted to implement that act;

5           (C) the Airline Deregulation Act, Pub. L. No. 95-504, only to the  
6           extent that an air carrier collects information related to prices, routes, or  
7           services, and only to the extent that the provisions of the Airline Deregulation  
8           Act preempt this chapter;

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

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

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

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

20           (14) a financial institution, credit union, independent trust company,  
21           broker-dealer, or investment adviser or a financial institution’s, credit union’s,

1 independent trust company’s, broker-dealer’s, or investment adviser’s affiliate  
2 or subsidiary that is only and directly engaged in financial activities, as  
3 described in 12 U.S.C. § 1843(k);

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

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

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

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

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

20 or

21 (20) noncommercial activity of:

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

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

6           (C) a nonprofit organization that provides programming to radio or  
7           television networks; or

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

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

14          § 2418. CONSUMER PERSONAL DATA RIGHTS

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

16           (1) confirm whether a controller is processing the consumer’s personal  
17           data and, if a controller is processing the consumer’s personal data, access the  
18           personal data;

19           (2) obtain from a controller a list of third parties to which the controller  
20           has disclosed the consumer’s personal data or, if the controller does not

1 maintain this information in a format specific to the consumer, a list of third  
2 parties to which the controller has disclosed personal data;

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

6 (4) delete personal data provided by, or obtained about, the consumer  
7 unless retention of the personal data is required by law;

8 (5) if the processing of personal data is done by automatic means, obtain  
9 a copy of the consumer’s personal data processed by the controller in a  
10 portable and, to the extent technically feasible, readily usable format that  
11 allows the consumer to transmit the data to another controller without  
12 hindrance; and

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

14 (A) targeted advertising;

15 (B) the sale of personal data; or

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

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

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

4           (3) A parent or legal guardian may exercise rights under this section on  
5           behalf of the parent’s child or on behalf of a child for whom the guardian has  
6           legal responsibility. A guardian or conservator may exercise the rights under  
7           this section on behalf of a consumer that is subject to a guardianship,  
8           conservatorship, or other protective arrangement.

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

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

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

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



1           (B) The controller may extend the response period by 45 additional  
2           days when reasonably necessary, considering the complexity and number of  
3           the consumer’s requests, provided the controller informs the consumer of the  
4           extension within the initial 45-day response period and of the reason for the  
5           extension.

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

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

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

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

19           (4)(A) If a controller is unable to authenticate a request to exercise any  
20           of the rights afforded under subdivisions (a)(1)–(5) of this section using  
21           commercially reasonable efforts, the controller shall not be required to comply

1 with a request to initiate an action pursuant to this section and shall provide  
2 notice to the consumer that the controller is unable to authenticate the request  
3 to exercise the right or rights until the consumer provides additional  
4 information reasonably necessary to authenticate the consumer and the  
5 consumer’s request to exercise the right or rights.

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

9 (C) If a controller denies an opt-out request because the controller  
10 believes the request is fraudulent, the controller shall send a notice to the  
11 person who made the request disclosing that the controller believes the request  
12 is fraudulent, why the controller believes the request is fraudulent, and that the  
13 controller shall not comply with the request.

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

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

1           (B) opting the consumer out of the processing of the personal data for  
2           any purpose except for those exempted pursuant to the provisions of this  
3           chapter.

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

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

8           (B) the employment of any dark pattern.

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

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

14          (2) Be conspicuously available to the consumer.

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

17          (4) Require the controller to approve or deny the appeal within 45 days  
18          after the date on which the controller received the appeal and to notify the  
19          consumer in writing of the controller’s decision and the reasons for the  
20          decision. If the controller denies the appeal, the notice must provide or specify

1 information that enables the consumer to contact the Attorney General to  
2 submit a complaint.

3 (e) Nothing in this section shall be construed to require a controller to  
4 reveal a trade secret.

5 § 2419. DUTIES OF CONTROLLERS

6 (a) A controller shall:

7 (1) limit the collection of personal data to what is reasonably necessary  
8 and proportionate to provide or maintain a specific product or service  
9 requested by the consumer to whom the data pertains;

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

14 (3) provide an effective mechanism for a consumer to revoke consent to  
15 the controller's processing of the consumer's personal data that is at least as  
16 easy as the mechanism by which the consumer provided the consumer's  
17 consent; and

18 (4) upon a consumer's revocation of consent to processing, cease to  
19 process the consumer's personal data as soon as practicable, but not later than  
20 15 days after receiving the request.

21 (b) A controller shall not:

1           (1) process personal data for a purpose not disclosed in the privacy  
2 notice required under subsection (d) of this section unless:

3           (A) the controller obtains the consumer’s consent; or

4           (B) the purpose is reasonably necessary to and compatible with a  
5 disclosed purpose;

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

9           (3) sell sensitive data;

10           (4) discriminate or retaliate against a consumer who exercises a right  
11 provided to the consumer under this chapter or refuses to consent to the  
12 processing of personal data for a separate product or service, including by:

13           (A) denying goods or services;

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

15           (C) providing a different level of quality or selection of goods or  
16 services to the consumer;

17           (5) process personal data in violation of State or federal laws that  
18 prohibit unlawful discrimination; or

19           (6)(A) except as provided in subdivision (B) of this subdivision (6).

20 process a consumer’s personal data in a manner that discriminates against

21 individuals or otherwise makes unavailable the equal enjoyment of goods or

1 services on the basis of an individual’s actual or perceived race, color, sex,  
2 sexual orientation or gender identity, physical or mental disability, religion,  
3 ancestry, or national origin;

4 (B) subdivision (A) of this subdivision (6) shall not apply to:

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

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

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

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

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

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

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

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

6           (ii) the consumer consents to the transfer.

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

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

11          (B) describes the controller’s purposes for processing the personal  
12          data;

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

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

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

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

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

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

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

14           (2) The privacy notice shall adhere to the accessibility and usability  
15           guidelines recommended under 42 U.S.C. chapter 126 (the Americans with  
16           Disabilities Act) and 29 U.S.C. 794d (section 508 of the Rehabilitation Act of  
17           1973), including ensuring readability for individuals with disabilities across  
18           various screen resolutions and devices and employing design practices that  
19           facilitate easy comprehension and navigation for all users.

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



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

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

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

14                   (A) does not unfairly disadvantage another controller;

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

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

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

1           (E)(i) enables the controller to reasonably determine whether the  
2           consumer has made a legitimate request pursuant to subsection 2418(b) of this  
3           title to opt out pursuant to subdivision 2418(a)(6) of this title; and

4           (ii) for purposes of subdivision (i) of this subdivision (C), use of  
5           an internet protocol address to estimate the consumer’s location shall be  
6           considered sufficient to accurately determine residency.

7           (f) If a consumer or authorized agent uses a method under subdivision  
8           (d)(1)(I) of this section to opt out of a controller’s processing of the  
9           consumer’s personal data pursuant to subdivision 2418(a)(6) of this title and  
10           the decision conflicts with a consumer’s voluntary participation in a bona fide  
11           reward, club card, or loyalty program or a program that provides premium  
12           features or discounts in return for the consumer’s consent to the controller’s  
13           processing of the consumer’s personal data, the controller may either comply  
14           with the request to opt out or notify the consumer of the conflict and ask the  
15           consumer to affirm that the consumer intends to withdraw from the bona fide  
16           reward, club card, or loyalty program or the program that provides premium  
17           features or discounts. If the consumer affirms that the consumer intends to  
18           withdraw, the controller shall comply with the request to opt out.

19           § 2420. DUTIES OF CONTROLLERS TO MINORS

20           (a)(1) A controller that offers any online service, product, or feature to a  
21           consumer whom the controller knows or consciously avoids knowing is a

1 minor shall use reasonable care to avoid any heightened risk of harm to minors  
2 caused by the online service, product, or feature.

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

6 (b) A controller that offers any online service, product, or feature to a  
7 consumer whom the controller knows or consciously avoids knowing is a  
8 minor shall not process the minor’s personal data for longer than is reasonably  
9 necessary to provide the online service, product, or feature.

10 (c) A controller that offers any online service, product, or feature to a  
11 consumer whom the controller knows or consciously avoids knowing is a  
12 minor and who has consented under section 2419(b)(2) to the processing of  
13 precise geolocation data shall:

14 (1) collect the minor’s precise geolocation data only as reasonably  
15 necessary for the controller to provide the online service, product, or feature;

16 and

17 (2) provide to the minor a conspicuous signal indicating that the  
18 controller is collecting the minor’s precise geolocation data and make the  
19 signal available to the minor for the entire duration of the collection of the  
20 minor’s precise geolocation data.

21 § 2421. DUTIES OF PROCESSORS

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

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

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

8                       (B) use appropriate technical and organizational measures to the  
9       extent reasonably practicable;

10               (2) adopt administrative, technical, and physical safeguards that are  
11       reasonably designed to protect the security and confidentiality of the personal  
12       data the processor processes, taking into account how the processor processes  
13       the personal data and the information available to the processor; and

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

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

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

19               (2) set forth clear instructions for processing data, the nature and  
20       purpose of the processing, the type of data that is subject to processing, and the  
21       duration of the processing;

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

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

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

9           (6) require the processor to make available to the controller, at the  
10          controller’s request, all information the controller needs to verify that the  
11          processor has complied with all obligations the processor has under this  
12          chapter;

13          (7) require the processor to enter into a subcontract with a person the  
14          processor engages to assist with processing personal data on the controller’s  
15          behalf and in the subcontract require the subcontractor to meet the processor’s  
16          obligations concerning personal data;

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

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

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

4           (9) prohibit the processor from combining personal data obtained from  
5 the controller with personal data that the processor:

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

7           (B) collects from an individual.

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

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

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

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

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

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

3           § 2422. DUTIES OF PROCESSORS TO MINORS

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

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

7                         (A) the nature of the processing;

8                         (B) the information available to the processor by appropriate  
9                         technical and organizational measures; and

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

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

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

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

1        (d) Determining whether a person is acting as a controller or processor with  
2        respect to a specific processing of data is a fact-based determination that  
3        depends upon the context in which personal data is to be processed. A person  
4        that is not limited in the person’s processing of personal data pursuant to a  
5        controller’s instructions, or that fails to adhere to the instructions, is a  
6        controller and not a processor with respect to a specific processing of data. A  
7        processor that continues to adhere to a controller’s instructions with respect to  
8        a specific processing of personal data remains a processor. If a processor  
9        begins, alone or jointly with others, determining the purposes and means of the  
10       processing of personal data, the processor is a controller with respect to the  
11       processing and may be subject to an enforcement action under section 2427 of  
12       this title.

13       § 2423. DATA PROTECTION ASSESSMENTS FOR PROCESSING

14                ACTIVITIES THAT PRESENT A HEIGHTENED RISK OF HARM  
15                TO A CONSUMER

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

19                (1) the processing of personal data for the purposes of targeted  
20        advertising;

21                (2) the sale of personal data;



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

3                   (A) unfair or deceptive treatment of, or unlawful disparate impact on,  
4           consumers;

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

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

9                   (D) other substantial injury to consumers; and

10           (4) the processing of sensitive data.

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

13                   (A) identify the categories of personal data processed, the purposes  
14           for processing the personal data, and whether the personal data is being  
15           transferred to third parties; and

16                   (B) identify and weigh the benefits that may flow, directly and  
17           indirectly, from the processing to the controller, the consumer, other  
18           stakeholders, and the public against the potential risks to the consumer  
19           associated with the processing, as mitigated by safeguards that can be  
20           employed by the controller to reduce the risks.

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

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

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

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

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

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

19          (e) If a controller conducts a data protection assessment for the purpose of  
20          complying with another applicable law or regulation, the data protection  
21          assessment shall be deemed to satisfy the requirements established in this

1 section if the data protection assessment is reasonably similar in scope and  
2 effect to the data protection assessment that would otherwise be conducted  
3 pursuant to this section.

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

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

8 § 2424. DATA PROTECTION ASSESSMENTS FOR ONLINE SERVICES,  
9 PRODUCTS, OR FEATURES OFFERED TO MINORS

10 (a) A controller that offers any online service, product, or feature to a  
11 consumer whom the controller knows or consciously avoids knowing is a  
12 minor shall conduct a data protection assessment for the online service product  
13 or feature:

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

16 (2) that addresses:

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

18 (B) the categories of a minor's personal data that the online service,  
19 product, or feature processes;

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

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

3           (b) A controller that conducts a data protection assessment pursuant to  
4           subsection (a) of this section shall review the data protection assessment as  
5           necessary to account for any material change to the processing operations of  
6           the online service, product, or feature that is the subject of the data protection  
7           assessment.

8           (c) If a controller conducts a data protection assessment pursuant to  
9           subsection (a) of this section or a data protection assessment review pursuant  
10           to subsection (b) of this section and determines that the online service, product,  
11           or feature that is the subject of the assessment poses a heightened risk of harm  
12           to a minor, the controller shall establish and implement a plan to mitigate or  
13           eliminate the heightened risk.

14           (d)(1) The Attorney General may require that a controller disclose any data  
15           protection assessment pursuant to subsection (a) of this section that is relevant  
16           to an investigation conducted by the Attorney General pursuant to section 2427  
17           of this title, and the controller shall make the data protection assessment  
18           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           (e) A single data protection assessment may address a comparable set of  
8           processing operations that include similar activities.

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

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

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

21          or

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

3           § 2425. DE-IDENTIFIED OR PSEUDONYMOUS DATA

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

5                 (1) take reasonable measures to ensure that the data cannot be used to  
6 re-identify an identified or identifiable individual or be associated with an  
7 individual or device that identifies or is linked or reasonably linkable to an  
8 individual or household;

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

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

13           (b) This section does not prohibit a controller from attempting to re-  
14 identify de-identified data solely for the purpose of testing the controller's  
15 methods for de-identifying data.

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

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

19                 (2) maintain data in identifiable form, or collect, obtain, retain, or access  
20 any data or technology, in order to associate a consumer with personal data in

1 order to authenticate the consumer’s request under subsection 2418(b) of this  
2 title; or

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

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

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

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

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

18 (e) A controller that discloses or transfers pseudonymous data or de-  
19 identified data shall exercise reasonable oversight to monitor compliance with  
20 any contractual commitments to which the pseudonymous data or de-identified

1 data is subject and shall take appropriate steps to address any breaches of those  
2 contractual commitments.

3 § 2426. CONSTRUCTION OF DUTIES OF CONTROLLERS AND  
4 PROCESSORS

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

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

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

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

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

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

19 (6) provide a product or service specifically requested by the consumer  
20 to whom the personal data pertains consistent with subdivision 2419(a)(1) of  
21 this title;



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

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

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

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

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

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

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

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

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

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

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

11           (2) effectuate a product recall; or

12           (3) identify and repair technical errors that impair existing or intended  
13           functionality.

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

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

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

4           (d)(1) A controller, processor, or consumer health data controller that  
5           discloses personal data to a processor or third-party controller pursuant to this  
6           chapter shall not be deemed to have violated this chapter if the processor or  
7           third-party controller that receives and processes the personal data violates this  
8           chapter, provided, at the time the disclosing controller, processor, or consumer  
9           health data controller disclosed the personal data, the disclosing controller,  
10           processor, or consumer health data controller did not have actual knowledge  
11           that the receiving processor or third-party controller would violate this chapter.

12           (2) A third-party controller or processor receiving personal data from a  
13           controller, processor, or consumer health data controller in compliance with  
14           this chapter is not in violation of this chapter for the transgressions of the  
15           controller, processor, or consumer health data controller from which the third-  
16           party controller or processor receives the personal data.

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

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

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

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

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

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

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

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

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

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

18          (B) Personal data collected, used, or retained pursuant to subsection  
19          (b) of this section shall be subject to reasonable administrative, technical, and  
20          physical measures to protect the confidentiality, integrity, and accessibility of

1 the personal data and to reduce reasonably foreseeable risks of harm to  
2 consumers relating to the collection, use, or retention of personal data.

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

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

11 (i) This chapter shall not be construed to require a controller, processor, or  
12 consumer health data controller to implement an age-verification or age-gating  
13 system or otherwise affirmatively collect the age of consumers. A controller,  
14 processor, or consumer health data controller that chooses to conduct  
15 commercially reasonable age estimation to determine which consumers are  
16 minors is not liable for an erroneous age estimation.

17 § 2427. ENFORCEMENT

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

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

5        (c)(1) If the Attorney General determines that a violation of this chapter or  
6        rules adopted pursuant to this chapter may be cured, the Attorney General may,  
7        prior to initiating any action for the violation, issue a notice of violation  
8        extending a 60-day cure period to the controller, processor, or consumer health  
9        data controller alleged to have violated this chapter or rules adopted pursuant  
10       to this chapter.

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

15                (A) the number of violations;

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

18                (C) the nature and extent of the controller's, processor's, or consumer  
19        health data controller's processing activities;

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

21                (E) the safety of persons or property;

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

3           (G) the sensitivity of the data.

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

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

7           (2) the nature of each violation;

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

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

12          § 2428. CONFIDENTIALITY OF CONSUMER HEALTH DATA

13          Except as provided in subsections 2417(a) and (b) of this title and section  
14          2426 of this title, no person shall:

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

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

20          (3) use a geofence to establish a virtual boundary that is within 1,850  
21          feet of any health care facility, including any mental health facility or

1 reproductive or sexual health facility, for the purpose of identifying, tracking,  
2 collecting data from, or sending any notification to a consumer regarding the  
3 consumer’s consumer health data.

4 Sec. 2. PUBLIC EDUCATION AND OUTREACH; ATTORNEY GENERAL  
5 STUDY

6 (a) The Attorney General shall implement a comprehensive public  
7 education, outreach, and assistance program for controllers and processors as  
8 those terms are defined in 9 V.S.A. § 2415. The program shall focus on:

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

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

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

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

16 (5) methods for conducting data inventories; and

17 (6) any other matters the Attorney General deems appropriate.

18 (b) The Attorney General shall provide guidance to controllers for  
19 establishing data privacy notices and opt-out mechanisms, which may be in the  
20 form of templates.



1        (c) The Attorney General shall implement a comprehensive public  
2        education, outreach, and assistance program for consumers as that term is  
3        defined in 9 V.S.A. § 2415. The program shall focus on:

4            (1) the rights afforded consumers under the Vermont Data Privacy Act,  
5        including:

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

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

8            (2) the obligations controllers have to consumers;

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

12           (4) understanding a privacy notice provided under the Act;

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

15           (6) any other matters the Attorney General deems appropriate.

16        (d) The Attorney General shall cooperate with states with comparable data  
17        privacy regimes to develop any outreach, assistance, and education programs,  
18        where appropriate.

19        (e) The Attorney General may have the assistance of the Vermont Law and  
20        Graduate School in developing education, outreach, and assistance programs  
21        under this section.

1       (f) On or before December 15, 2026, the Attorney General shall assess the  
2       effectiveness of the implementation of the Act and submit a report to the  
3       House Committee on Commerce and Economic Development and the Senate  
4       Committee on Economic Development, Housing and General Affairs with its  
5       findings and recommendations, including any proposed draft legislation to  
6       address issues that have arisen since implementation.

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

8                   CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

9                                   Subchapter 1. General Provisions

10       § 2430. DEFINITIONS

11       As used in this chapter:

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

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

17                   (i) name;

18                   (ii) address;

19                   (iii) date of birth;

20                   (iv) place of birth;

21                   (v) mother’s maiden name;

1                   (vi) ~~unique biometric data generated from measurements or~~  
2 ~~technical analysis of human body characteristics used by the owner or licensee~~  
3 ~~of the data to identify or authenticate the consumer, such as a fingerprint, retina~~  
4 ~~or iris image, or other unique physical representation or digital representation~~  
5 ~~of biometric data;~~

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

8                   (viii) Social Security number or other government-issued  
9 identification number; or

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

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

16                  ~~(2)~~(3) “Business” means a controller, a consumer health data controller,  
17 a processor, or a commercial entity, including a sole proprietorship,  
18 partnership, corporation, association, limited liability company, or other group,  
19 however organized and whether or not organized to operate at a profit,  
20 including a financial institution organized, chartered, or holding a license or  
21 authorization certificate under the laws of this State, any other state, the United

1 States, or any other country, or the parent, affiliate, or subsidiary of a financial  
2 institution, but does not include the State, a State agency, any political  
3 subdivision of the State, or a vendor acting solely on behalf of, and at the  
4 direction of, the State.

5 ~~(3)~~(4) “Consumer” means an individual residing in this State.

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

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

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

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

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

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

18 (iii) investor in the business; or

19 (iv) donor to the business.

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

4 (i) developing or maintaining third-party e-commerce or  
5 application platforms;

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

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

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

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

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

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

19 ~~(5)(8)~~(A) “Data broker security breach” means an unauthorized  
20 acquisition or a reasonable belief of an unauthorized acquisition of more than  
21 one element of brokered personal information maintained by a data broker

1 when the brokered personal information is not encrypted, redacted, or  
2 protected by another method that renders the information unreadable or  
3 unusable by an unauthorized person.

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

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

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

17 (ii) indications that the brokered personal information has been  
18 downloaded or copied;

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

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

2 ~~(6)~~(9) “Data collector” means a person who, for any purpose, whether  
3 by automated collection or otherwise, handles, collects, disseminates, or  
4 otherwise deals with personally identifiable information, and includes the  
5 State, State agencies, political subdivisions of the State, public and private  
6 universities, privately and publicly held corporations, limited liability  
7 companies, financial institutions, and retail operators.

8 ~~(7)~~(10) “Encryption” means use of an algorithmic process to transform  
9 data into a form in which the data is rendered unreadable or unusable without  
10 use of a confidential process or key.

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

15 ~~(9)~~(12) “Login credentials” means a consumer’s user name or e-mail  
16 address, in combination with a password or an answer to a security question,  
17 that together permit access to an online account.

18 ~~(10)~~(13)(A) “Personally identifiable information” means a consumer’s  
19 first name or first initial and last name in combination with one or more of the  
20 following digital data elements, when the data elements are not encrypted,

1 redacted, or protected by another method that renders them unreadable or  
2 unusable by unauthorized persons:

3 (i) a Social Security number;

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

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

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

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

19 (vi) genetic information; and

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



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

3 (III) a health insurance policy number.

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

7 (14) “Processor” has the same meaning as in section 2415 of this title.

8 ~~(14)~~(15) “Record” means any material on which written, drawn, spoken,  
9 visual, or electromagnetic information is recorded or preserved, regardless of  
10 physical form or characteristics.

11 ~~(15)~~(16) “Redaction” means the rendering of data so that the data are  
12 unreadable or are truncated so that ~~no~~ not more than the last four digits of the  
13 identification number are accessible as part of the data.

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

19 (B) “Security breach” does not include good faith but unauthorized  
20 acquisition of personally identifiable information or login credentials by an  
21 employee or agent of the data collector for a legitimate purpose of the data

1 collector, provided that the personally identifiable information or login  
2 credentials are not used for a purpose unrelated to the data collector’s business  
3 or subject to further unauthorized disclosure.

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

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

11 (ii) indications that the information has been downloaded or  
12 copied;

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

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

17 \* \* \*

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

19 \* \* \*

20 § 2436. NOTICE OF DATA BROKER SECURITY BREACH

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

3        (b) Notice of breach.

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

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

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

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

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

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

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

19          (3) The notice to a consumer required by this subsection shall be  
20 delayed upon request of a law enforcement agency. A law enforcement agency  
21 may request the delay if it believes that notification may impede a law

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

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

19 (A) the incident in general terms;

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

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

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

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

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

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

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

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

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

20           (ii) the notice is consistent with the provisions regarding electronic  
21 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  
3 title 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 a consumer to opt out of the data  
16 broker's collection of brokered personal information, opt out of its databases,  
17 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) 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, sales activities, and opt-out policies that  
13 are applicable to the brokered personal information of minors; and

14 (G) 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 30 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 30 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; CREDENTIALING

18 (a) Credentialing.

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

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

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

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

10       Sec. 4. STUDY; DATA BROKERS; OPT OUT

11       On or before January 1, 2025, the Secretary of State, in collaboration with  
12       the Agency of Digital Services, the Attorney General, and interested parties,  
13       shall review and report their findings and recommendations to the House  
14       Committee on Commerce and Economic Development and the Senate  
15       Committee on Economic Development, Housing and General Affairs  
16       concerning one or more mechanisms for Vermont consumers to opt out of the  
17       collection, retention, and sale of brokered personal information, including:

18           (1) an individual opt out that requires a data broker to allow a consumer  
19           to opt out of its data collection, retention, and sales practices through a request  
20           made directly to the data broker; and

1           (2) specifically considering the rules, procedures, and framework for  
2           implementing the “accessible deletion mechanism” by the California Privacy  
3           Protection Agency that takes effect on January 1, 2026, and approaches in  
4           other jurisdictions if applicable:

5           (A) how to design and implement a State-facilitated general opt out  
6           mechanism;

7           (B) the associated implementation and operational costs;

8           (C) mitigation of security risks; and

9           (D) other relevant considerations.

10          Sec. 5. 9 V.S.A. § 2416(a) is amended to read:

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

15               (1) controlled or processed the personal data of not fewer than ~~25,000~~  
16               12,500 consumers, excluding personal data controlled or processed solely for  
17               the purpose of completing a payment transaction; or

18               (2) controlled or processed the personal data of not fewer than ~~12,500~~  
19               6,250 consumers and derived more than ~~25~~ 20 percent of the person’s gross  
20               revenue from the sale of personal data.

1 Sec. 6. 9 V.S.A. § 2416(a) is amended to read:

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

6 (1) controlled or processed the personal data of not fewer than ~~12,500~~  
7 6,250 consumers, excluding personal data controlled or processed solely for  
8 the purpose of completing a payment transaction; or

9 (2) controlled or processed the personal data of not fewer than ~~6,250~~  
10 3,125 consumers and derived more than 20 percent of the person's gross  
11 revenue from the sale of personal data.

12 Sec. 7. 9 V.S.A. § 2427 is amended to read:

13 § 2427. ENFORCEMENT

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

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

1       ~~(c)(1) If the Attorney General determines that a violation of this chapter or~~  
2       ~~rules adopted pursuant to this chapter may be cured, the Attorney General may,~~  
3       ~~prior to initiating any action for the violation, issue a notice of violation~~  
4       ~~extending a 60-day cure period to the controller, processor, or consumer health~~  
5       ~~data controller alleged to have violated this chapter or rules adopted pursuant~~  
6       ~~to this chapter.~~

7       ~~(2) The Attorney General may, in determining whether to grant a~~  
8       ~~controller, processor, or consumer health data controller the opportunity to~~  
9       ~~cure an alleged violation described in subdivision (1) of this subsection,~~  
10       ~~consider:~~

11               ~~(A) the number of violations;~~

12               ~~(B) the size and complexity of the controller, processor, or consumer~~  
13       ~~health data controller;~~

14               ~~(C) the nature and extent of the controller's, processor's, or consumer~~  
15       ~~health data controller's processing activities;~~

16               ~~(D) the substantial likelihood of injury to the public;~~

17               ~~(E) the safety of persons or property;~~

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

20               ~~(G) the sensitivity of the data.~~

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

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

4           ~~(2) the nature of each violation;~~

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

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

9       Sec. 8. 9 V.S.A. § 2427 is amended to read:

10       § 2427. ENFORCEMENT AND PRIVATE RIGHT OF ACTION

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

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

18       (c)(1) A consumer who is harmed by a controller's, processor's, or  
19 consumer health data controller's violation of subdivision 2419(b)(2) of this  
20 title, subdivision 2419(b)(3) of this title, or section 2428 of this title may bring



1 an action in Superior Court against the controller, processor, or consumer  
2 health data controller for the alleged violation if:

3 (A) the consumer notifies the controller, processor, or consumer  
4 health data controller of the violation; and

5 (B)(i) the controller, processor, or consumer health data controller  
6 fails to cure the violation within 60 days following receipt of the notice of  
7 violation; or

8 (ii) no cure is possible.

9 (2) A consumer bringing an action under this subsection may seek:

10 (A) the greater of \$1,000.00 or actual damages;

11 (B) injunctive relief;

12 (C) punitive damages in the case of an intentional violation; and

13 (D) reasonable costs and attorney's fees.

14 (d) Annually, on or before February 1, the Attorney General shall submit a  
15 report to the General Assembly disclosing:

16 (1) the number of actions brought under subsection (c) of this section;

17 (2) the number of violations asserted, broken down by statutory basis;

18 (3) the proportion of actions brought under subsection (c) of this section  
19 that proceed to trial;

20 (4) the controllers, processors, or consumer health data controllers most  
21 frequently sued under subsection (c) of this section; and

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

3           Sec. 9. 9 V.S.A. § 2427 is amended to read:

4           § 2427. ENFORCEMENT AND PRIVATE RIGHT OF ACTION

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

8           (b) The Attorney General has the same authority to adopt rules to  
9           implement the provisions of this section and to conduct civil investigations,  
10          enter into assurances of discontinuance, bring civil actions, and take other  
11          enforcement actions as provided under chapter 63, subchapter 1 of this title.

12          ~~(c)(1) A consumer who is harmed by a controller's, processor's, or~~  
13          ~~consumer health data controller's violation of subdivision 2419(b)(2) of this~~  
14          ~~title, subdivision 2419(b)(3) of this title, or section 2428 of this title may bring~~  
15          ~~an action in Superior Court against the controller, processor, or consumer~~  
16          ~~health data controller for the alleged violation if:~~

17                  ~~(A) the consumer notifies the controller, processor, or consumer~~  
18          ~~health data controller of the violation; and~~

19                  ~~(B)(i) the controller, processor, or consumer health data controller~~  
20          ~~fails to cure the violation within 60 days following receipt of the notice of~~  
21          ~~violation; or~~

1           ~~(ii) no cure is possible.~~

2           ~~(2) A consumer bringing an action under this subsection may seek:~~

3                 ~~(A) the greater of \$1,000.00 or actual damages;~~

4                 ~~(B) injunctive relief;~~

5                 ~~(C) punitive damages in the case of an intentional violation; and~~

6                 ~~(D) reasonable costs and attorney's fees.~~

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

9                 ~~(1) the number of actions brought under subsection (c) of this section;~~

10                ~~(2) the number of violations asserted, broken down by statutory basis;~~

11                ~~(3) the proportion of actions brought under subsection (c) of this section~~  
12 ~~that proceed to trial;~~

13                ~~(4) the controllers, processors, or consumer health data controllers most~~  
14 ~~frequently sued under subsection (c) of this section; and~~

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

17           Sec. 10. 9 V.S.A. chapter 62, subchapter 6 is added to read:

18                         Subchapter 6. Age-Appropriate Design Code

19           § 2449a. DEFINITIONS

20           As used in this subchapter:

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

4           (B) As used in subdivision (A) of this subdivision (1), “control” or  
5           “controlled” means:

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

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

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

12           (2) “Age-appropriate” means a recognition of the distinct needs and  
13           diversities of minor consumers at different age ranges. In order to help support  
14           the design of online services, products, and features, covered businesses should  
15           take into account the unique needs and diversities of different age ranges,  
16           including the following developmental stages: zero to five years of age or  
17           “preliterate and early literacy”; six to nine years of age or “core primary school  
18           years”; 10 to 12 years of age or “transition years”; 13 to 15 years of age or  
19           “early teens”; and 16 to 17 years of age or “approaching adulthood.”

20           (3) “Age estimation” means a process that estimates that a user is likely  
21           to be of a certain age, fall within an age range, or is over or under a certain age.

1           (A) Age estimation methods include:

2                   (i) analysis of behavioral and environmental data the covered

3 business already collects about its users;

4                   (ii) comparing the way a user interacts with a device or with users

5 of the same age;

6                   (iii) metrics derived from motion analysis; and

7                   (iv) testing a user’s capacity or knowledge.

8           (B) Age estimation does not require certainty, and if a covered

9 business estimates a user’s age for the purpose of advertising or marketing, that

10 estimation may also be used to comply with this act.

11           (4) “Age verification” means a system that relies on hard identifiers or

12 verified sources of identification to confirm a user has reached a certain age,

13 including government-issued identification or a credit card.

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

15           (6) “Collect” means buying, renting, gathering, obtaining, receiving, or

16 accessing any personal data by any means. This includes receiving data from

17 the consumer, either actively or passively, or by observing the consumer’s

18 behavior.

19           (7)(A) “Consumer” means an individual who is a Vermont resident.

20                   (B) “Consumer” does not include an individual acting in a

21 commercial or employment context or as an employee, owner, director, officer,

1 or contractor of a company, partnership, sole proprietorship, nonprofit, or  
2 government agency whose communications or transactions with the covered  
3 business occur solely within the context of that individual’s role with the  
4 company, partnership, sole proprietorship, nonprofit, or government agency.

5 (8) “Covered business” means a sole proprietorship, partnership, limited  
6 liability company, corporation, association, other legal entity, or an affiliate  
7 thereof, that conducts business in this State or that produces online products,  
8 services, or features that are targeted to residents of this State and that:

9 (A) collects consumers’ personal data or has consumers’ personal  
10 data collected on its behalf by a third party;

11 (B) alone or jointly with others determines the purposes and means of  
12 the processing of consumers personal data; and

13 (C) alone or in combination annually buys, receives for commercial  
14 purposes, sells, or shares for commercial purposes, alone or in combination,  
15 the personal data of at least 50 percent of its consumers.

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

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

1           (11) “Default” means a preselected option adopted by the covered  
2           business for the online service, product, or feature.

3           (12) “Deidentified” means data that cannot reasonably be used to infer  
4           information about, or otherwise be linked to, an identified or identifiable  
5           consumer, or a device linked to such consumer, provided that the covered  
6           business that possesses the data:

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

9                   (B) publicly commits to maintain and use the data only in a  
10                  deidentified fashion and not attempt to reidentify the data; and

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

13           (13) “Derived data” means data that is created by the derivation of  
14           information, data, assumptions, correlations, inferences, predictions, or  
15           conclusions from facts, evidence, or another source of information or data  
16           about a minor consumer or a minor consumer’s device.

17           (14)(A) “Low-friction variable reward” means a design feature or  
18           virtual item that intermittently rewards consumers for scrolling, tapping,  
19           opening, or continuing to engage in an online service, product, or feature.

20                   (B) Examples of low-friction variable reward designs include  
21           endless scroll, auto play, and nudges meant to encourage reengagement.

1           (15)(A) “Minor consumer” means an individual under 18 years of age  
2           who is a Vermont resident.

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

9           (16) “Online service, product, or feature” means a digital product that is  
10           accessible to the public via the internet, including a website or application, and  
11           does not mean any of the following:

12                   (A) telecommunications service, as defined in 47 U.S.C. § 153;

13                   (B) a broadband internet access service as defined in 47 C.F.R.  
14                   § 54.400; or

15                   (C) the sale, delivery, or use of a physical product.

16           (17) “Personal data” means any information, including derived data and  
17           unique identifiers, that is linked or reasonably linkable, alone or in  
18           combination with other information, to an identified or identifiable individual  
19           or to a device that identifies, is linked to, or is reasonably linkable to one or  
20           more identified or identifiable individuals in a household. Personal data does  
21           not include deidentified data or publicly available information.



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

5           (19) “Processor” means a person who processes personal data on behalf  
6           of a covered business.

7           (20) “Profile” or “profiling” means any form of automated processing of  
8           personal data to evaluate, analyze, or predict personal aspects concerning an  
9           identified or identifiable consumer’s economic situation, health, personal  
10           preferences, interests, reliability, behavior, location, or movements.

11           (21) “Publicly available information” means information that:

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

14           (B) a covered business has a reasonable basis to believe that the  
15           consumer has lawfully made available to the general public through widely  
16           distributed media.

17           (22) “Reasonably likely to be accessed” means an online service,  
18           product, or feature that is likely to be accessed by minor consumers based on  
19           any of the following indicators:

1           (A) the online service, product, or feature is directed to children, as  
2           defined by the Children’s Online Privacy Protection Act, 15 U.S.C. §§ 6501–  
3           6506 and the Federal Trade Commission rules implementing that Act;

4           (B) the online service, product, or feature is determined, based on  
5           competent and reliable evidence regarding audience composition, to be  
6           routinely accessed by an audience that is composed of at least two percent  
7           minor consumers two through under 18 years of age;

8           (C) the online service, product, or feature contains advertisements  
9           marketed to minor consumers;

10           (D) the audience of the online service, product, or feature is  
11           determined, based on internal company research, to be composed of at least  
12           two percent minor consumers two through under 18 years of age; or

13           (E) the covered business knew or should have known that at least two  
14           percent of the audience of the online service, product, or feature includes  
15           minor consumers two through under 18 years of age, provided that, in making  
16           this assessment, the business shall not collect or process any personal data that  
17           is not reasonably necessary to provide an online service, product, or feature  
18           with which a minor consumer is actively and knowingly engaged.

19           (23)(A) “Social media platform” means a public or semi-public internet-  
20           based service or application that is primarily intended to connect and allow a

1 user to socially interact within such service or application and enables a user  
2 to:

3 (i) construct a public or semi-public profile for the purposes of  
4 signing into and using such service or application;

5 (ii) populate a public list of other users with whom the user shares  
6 a social connection within such service or application; or

7 (iii) create or post content that is viewable by other users,  
8 including content on message boards and in chat rooms, and that presents the  
9 user with content generated by other users.

10 (B) “Social media platform” does not mean a public or semi-public  
11 internet-based service or application that:

12 (i) exclusively provides electronic mail or direct messaging  
13 services;

14 (ii) primarily consists of news, sports, entertainment, interactive  
15 video games, electronic commerce, or content that is preselected by the  
16 provider for which any interactive functionality is incidental to, directly related  
17 to, or dependent on the provision of such content; or

18 (iii) is used by and under the direction of an educational entity,  
19 including a learning management system or a student engagement program.

20 (24) “Third party” means a natural or legal person, public authority,  
21 agency, or body other than the consumer or the covered business.

1     § 2449b. EXCLUSIONS

2             This subchapter does not apply to:

3                 (1) a federal, state, tribal, or local government entity in the ordinary  
4     course of its operation;

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

8                 (3) information used only for public health activities and purposes  
9     described in 45 C.F.R. § 164.512;

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

11                    (A) activities that are subject to the Federal Policy for the Protection  
12     of Human Subjects as set forth in 45 C.F.R. Part 46;

13                    (B) research on human subjects undertaken in accordance with good  
14     clinical practice guidelines issued by the International Council for  
15     Harmonisation of Technical Requirements for Pharmaceuticals for Human  
16     Use;

17                    (C) activities that are subject to the protections provided in 21 C.F.R.  
18     50 and 21 C.F.R. Part 56; or

19                    (D) research conducted in accordance with the requirements set forth  
20     in subdivisions (A)–(C) of this subdivision (4) or otherwise in accordance with  
21     State or federal law; and

1           (5) an entity whose primary purpose is journalism as defined in  
2           12 V.S.A. § 1615(a)(2) and that has a majority of its workforce consisting of  
3           individuals engaging in journalism.

4           § 2449c. MINIMUM DUTY OF CARE

5           (a) A covered business that processes a minor consumer’s data in any  
6           capacity owes a minimum duty of care to the minor consumer.

7           (b) As used in this subchapter, “a minimum duty of care” means the use of  
8           the personal data of a minor consumer and the design of an online service,  
9           product, or feature will not benefit the covered business to the detriment of a  
10           minor consumer and will not result in:

11           (1) reasonably foreseeable emotional distress as defined in 13 V.S.A.  
12           § 1061(2) to a minor consumer;

13           (2) the encouragement of excessive or compulsive use of the online  
14           service, product, or feature by a minor consumer; or

15           (3) discrimination against the minor consumer based upon race,  
16           ethnicity, sex, disability, sexual orientation, gender identity, gender expression,  
17           or national origin.

18           § 2449d. COVERED BUSINESS OBLIGATIONS

19           (a) A covered business that is reasonably likely to be accessed and subject  
20           to this subchapter shall:

1           (1) configure all default privacy settings provided to a minor consumer  
2           through the online service, product, or feature to a high level of privacy;

3           (2) provide privacy information, terms of service, policies, and  
4           community standards concisely and prominently;

5           (3) provide prominent, accessible, and responsive tools to help a minor  
6           consumer or, if applicable, their parents or guardians to exercise their privacy  
7           rights and report concerns to the covered business;

8           (4) honor the request of a minor consumer to unpublish the minor  
9           consumer’s social media platform account not later than 15 business days after  
10           a covered business receives such a request from a minor consumer; and

11           (5) provide easily accessible and age-appropriate tools for a minor  
12           consumer to limit the ability of users or covered businesses to send unsolicited  
13           communications.

14           (b) A violation of this section constitutes a violation of the minimum duty  
15           of care as provided in section 2449c of this subchapter.

16           § 2449e. COVERED BUSINESS PROHIBITIONS

17           (a) A covered business that is reasonably likely to be accessed and subject  
18           to this subchapter shall not:

19           (1) use low-friction variable reward design features that encourage  
20           excessive and compulsive use by a minor consumer;

1           (2) permit, by default, an unknown adult to contact a minor consumer on  
2           its platform without the minor consumer first initiating that contact;

3           (3) permit a minor consumer to be exploited by a contract on the online  
4           service, product, or feature;

5           (4) use dark patterns; or

6           (5) permit a parent or guardian of a minor consumer, or any other  
7           consumer, to monitor the online activity of a minor consumer or to track the  
8           location of the minor consumer without providing a conspicuous signal to the  
9           minor consumer when the minor consumer is being monitored or tracked.

10          (b) A violation of this section constitutes a violation of the minimum duty  
11          of care as provided in section 2449c of this subchapter.

12          § 2449f. ATTORNEY GENERAL ENFORCEMENT

13          (a) A covered business that violates this subchapter or rules adopted  
14          pursuant to this subchapter commits an unfair and deceptive act in  
15          commerce in violation of section 2453 of this title.

16          (b) The Attorney General shall have the same authority under this  
17          subchapter to make rules, conduct civil investigations, bring civil actions,  
18          and enter into assurances of discontinuance as provided under chapter 63 of  
19          this title.

20          § 2449g. LIMITATIONS

21          Nothing in this subchapter shall be interpreted or construed to:

1           (1) Impose liability in a manner that is inconsistent with 47 U.S.C.  
2           § 230.

3           (2) Prevent or preclude any minor consumer from deliberately or  
4           independently searching for, or specifically requesting, content.

5           (3) Require a covered business to implement an age verification  
6           requirement. The obligations imposed under this act should be done with age  
7           estimation techniques and do not require age verification.

8           § 2449h. RIGHTS AND FREEDOMS OF MINOR CONSUMERS

9           It is the intent of the General Assembly that nothing in this act may be  
10           construed to infringe on the existing rights and freedoms of minor consumers  
11           or be construed to discriminate against the minor consumer based on race,  
12           ethnicity, sex, disability, sexual orientation, gender identity, gender expression,  
13           or national origin.

14           Sec. 11. EFFECTIVE DATES

15           (a) This section and Secs. 2 (public education and outreach), 3 (protection  
16           of personal information), and 4 (data broker opt-out study) shall take effect on  
17           July 1, 2024.

18           (b) Secs. 1 (Vermont Data Privacy Act) and 10 (Age-Appropriate Design  
19           Code) shall take effect on July 1, 2025.

20           (c) Secs. 5 (Vermont Data Privacy Act middle applicability threshold) and  
21           8 (private right of action) shall take effect on July 1, 2026.



1           (d) Sec. 7 (cure period phase out) shall take effect on January 1, 2027.

2           (e) Sec. 6 (Vermont Data Privacy Act low applicability threshold) shall  
3 take effect on July 1, 2027.

4           (f) Sec. 9 (private right of action phase out) shall take effect on July 1,  
5 2029.

6           and that after passage the title of the bill be amended to read: “An act  
7 relating to enhancing consumer privacy and the age-appropriate design code.”

8

9

10

11           (Committee vote: \_\_\_\_\_)

12

\_\_\_\_\_

13

Representative \_\_\_\_\_

14

FOR THE COMMITTEE