H.121 Page 1 of 98

1	H.121
2	An act relating to enhancing consumer privacy
3	The House concurs in the Senate proposal of amendment with further
4	proposal of amendment thereto by striking out all after the enacting clause and
5	inserting in lieu thereof the following:
6	Sec. 1. 9 V.S.A. chapter 61A is added to read:
7	CHAPTER 61A. VERMONT DATA PRIVACY ACT
8	§ 2415. DEFINITIONS
9	As used in this chapter:
10	(1)(A) "Affiliate" means a legal entity that shares common branding
11	with another legal entity or controls, is controlled by, or is under common
12	control with another legal entity.
13	(B) As used in subdivision (A) of this subdivision (1), "control" or
14	"controlled" means:
15	(i) ownership of, or the power to vote, more than 50 percent of the
16	outstanding shares of any class of voting security of a company;
17	(ii) control in any manner over the election of a majority of the
18	directors or of individuals exercising similar functions; or
19	(iii) the power to exercise controlling influence over the
20	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.

H.121 Page 3 of 98

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.

H.121 Page 4 of 98

1	(9)(A) "Consent" means a clear affirmative act signifying a consumer's
2	freely given, specific, informed, and unambiguous agreement to allow the
3	processing of personal data relating to the consumer.
4	(B) "Consent" may include a written statement, including by
5	electronic means, or any other unambiguous affirmative action.
6	(C) "Consent" does not include:
7	(i) acceptance of a general or broad terms of use or similar
8	document that contains descriptions of personal data processing along with
9	other, unrelated information;
10	(ii) hovering over, muting, pausing, or closing a given piece of
11	content; or
12	(iii) agreement obtained through the use of dark patterns.
13	(10)(A) "Consumer" means an individual who is a resident of the State.
14	(B) "Consumer" does not include an individual acting in a
15	commercial or employment context or as an employee, owner, director, officer,
16	or contractor of a company, partnership, sole proprietorship, nonprofit, or
17	government agency whose communications or transactions with the controller
18	occur solely within the context of that individual's role with the company,
19	partnership, sole proprietorship, nonprofit, or government agency.

H.121 Page 5 of 98

1	(11) "Consumer health data" means any personal data that a controller
2	uses to identify a consumer's physical or mental health condition or diagnosis,
3	including gender-affirming health data and reproductive or sexual health data.
4	(12) "Consumer health data controller" means any controller that, alone
5	or jointly with others, determines the purpose and means of processing
6	consumer health data.
7	(13) "Consumer reporting agency" has the same meaning as in the Fair
8	Credit Reporting Act, 15 U.S.C. § 1681a(f);
9	(14) "Controller" means a person who, alone or jointly with others,
10	determines the purpose and means of processing personal data.
11	(15) "COPPA" means the Children's Online Privacy Protection Act of
12	1998, 15 U.S.C. § 6501-6506, and any regulations, rules, guidance, and
13	exemptions promulgated pursuant to the act, as the act and regulations, rules,
14	guidance, and exemptions may be amended.
15	(16) "Covered entity" has the same meaning as in HIPAA.
16	(17) "Credit union" has the same meaning as in 8 V.S.A. § 30101.
17	(18) "Dark pattern" means a user interface designed or manipulated with
18	the substantial effect of subverting or impairing user autonomy, decision-
19	making, or choice and includes any practice the Federal Trade Commission
20	refers to as a "dark pattern."

	I	H.1	21
Page	6	of	98

1	(19) "Data broker" has the same meaning as in section 2430 of this title.
2	(20) "Decisions that produce legal or similarly significant effects
3	concerning the consumer" means decisions made by the controller that result in
4	the provision or denial by the controller of financial or lending services,
5	housing, insurance, education enrollment or opportunity, criminal justice,
6	employment opportunities, health care services, or access to essential goods or
7	services.
8	(21) "De-identified data" means data that does not identify and cannot
9	reasonably be used to infer information about, or otherwise be linked to, an
10	identified or identifiable individual, or a device linked to the individual, if the
11	controller that possesses the data:
12	(A)(i) takes reasonable measures to ensure that the data cannot be
13	used to re-identify an identified or identifiable individual or be associated with
14	an individual or device that identifies or is linked or reasonably linkable to an
15	individual or household;
16	(ii) for purposes of this subdivision (A), "reasonable measures"
17	shall include the de-identification requirements set forth under 45 C.F.R.
18	§ 164.514 (other requirements relating to uses and disclosures of protected
19	health information);

H.121 Page 7 of 98

1	(B) publicly commits to process the data only in a de-identified
2	fashion and not attempt to re-identify the data; and
3	(C) contractually obligates any recipients of the data to satisfy the
4	criteria set forth in subdivisions (A) and (B) of this subdivision (21).
5	(22) "Financial institution":
6	(A) as used in subdivision 2417(a)(12) of this title, has the same
7	meaning as in 15 U.S.C. § 6809; and
8	(B) as used in subdivision 2417(a)(14) of this title, has the same
9	meaning as in 8 V.S.A. § 11101.
10	(23) "Gender-affirming health care services" has the same meaning as in
11	<u>1 V.S.A. § 150.</u>
12	(24) "Gender-affirming health data" means any personal data
13	concerning a past, present, or future effort made by a consumer to seek, or a
14	consumer's receipt of, gender-affirming health care services, including:
15	(A) precise geolocation data that is used for determining a
16	consumer's attempt to acquire or receive gender-affirming health care services;
17	(B) efforts to research or obtain gender-affirming health care
18	services; and
19	(C) any gender-affirming health data that is derived from nonhealth
20	information.

1	(25) "Genetic data" means any data, regardless of its format, that results
2	from the analysis of a biological sample of an individual, or from another
3	source enabling equivalent information to be obtained, and concerns genetic
4	material, including deoxyribonucleic acids (DNA), ribonucleic acids (RNA),
5	genes, chromosomes, alleles, genomes, alterations or modifications to DNA or
6	RNA, single nucleotide polymorphisms (SNPs), epigenetic markers,
7	uninterpreted data that results from analysis of the biological sample or other
8	source, and any information extrapolated, derived, or inferred therefrom.
9	(26) "Geofence" means any technology that uses global positioning
10	coordinates, cell tower connectivity, cellular data, radio frequency
11	identification, wireless fidelity technology data, or any other form of location
12	detection, or any combination of such coordinates, connectivity, data,
13	identification, or other form of location detection, to establish a virtual
14	boundary.
15	(27) "Health care facility" has the same meaning as in 18 V.S.A. § 9432.
16	(28) "Heightened risk of harm to a minor" means processing the
17	personal data of a minor in a manner that presents a reasonably foreseeable risk
18	of:
19	(A) unfair or deceptive treatment of, or unlawful disparate impact on,
20	a minor;

	ŀ	H.12	21
Page	9	of 9	8

1	(B) financial, physical, or reputational injury to a minor;
2	(C) unintended disclosure of the personal data of a minor; or
3	(D) any physical or other intrusion upon the solitude or seclusion, or
4	the private affairs or concerns, of a minor if the intrusion would be offensive to
5	a reasonable person.
6	(29) "HIPAA" means the Health Insurance Portability and
7	Accountability Act of 1996, Pub. L. No. 104-191, and any regulations
8	promulgated pursuant to the act, as may be amended.
9	(30) "Identified or identifiable individual" means an individual who can
10	be readily identified, directly or indirectly, including by reference to an
11	identifier such as a name, an identification number, specific geolocation data,
12	or an online identifier.
13	(31) "Independent trust company" has the same meaning as in 8 V.S.A.
14	<u>§ 2401.</u>
15	(32) "Investment adviser" has the same meaning as in 9 V.S.A. § 5102.
16	(33) "Large data holder" means a person that during the preceding
17	calendar year processed the personal data of not fewer than 100,000
18	consumers.

1	(34) "Mental health facility" means any health care facility in which at
2	least 70 percent of the health care services provided in the facility are mental
3	health services.
4	(35) "Nonpublic personal information" has the same meaning as in
5	15 U.S.C. § 6809.
6	(36)(A) "Online service, product, or feature" means any service,
7	product, or feature that is provided online, except as provided in subdivision
8	(B) of this subdivision (36).
9	(B) "Online service, product, or feature" does not include:
10	(i) telecommunications service, as that term is defined in the
11	Communications Act of 1934, 47 U.S.C. § 153;
12	(ii) broadband internet access service, as that term is defined in
13	47 C.F.R. § 54.400 (universal service support); or
14	(iii) the delivery or use of a physical product.
15	(37) "Patient identifying information" has the same meaning as in
16	42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).
17	(38) "Patient safety work product" has the same meaning as in 42 C.F.R.
18	§ 3.20 (patient safety organizations and patient safety work product).
19	(39)(A) "Personal data" means any information, including derived data
20	and unique identifiers, that is linked or reasonably linkable to an identified or

H.121 Page 11 of 98

1	identifiable individual or to a device that identifies, is linked to, or is
2	reasonably linkable to one or more identified or identifiable individuals in a
3	household.
4	(B) "Personal data" does not include de-identified data or publicly
5	available information.
6	(40)(A) "Precise geolocation data" means information derived from
7	technology that can precisely and accurately identify the specific location of a
8	consumer within a radius of 1,850 feet.
9	(B) "Precise geolocation data" does not include:
10	(i) the content of communications;
11	(ii) data generated by or connected to an advanced utility metering
12	infrastructure system; or
13	(iii) data generated by equipment used by a utility company.
14	(41) "Process" or "processing" means any operation or set of operations
15	performed, whether by manual or automated means, on personal data or on sets
16	of personal data, such as the collection, use, storage, disclosure, analysis,
17	deletion, or modification of personal data.
18	(42) "Processor" means a person who processes personal data on behalf
19	of a controller.

1	(43) "Profiling" means any form of automated processing performed on
2	personal data to evaluate, analyze, or predict personal aspects related to an
3	identified or identifiable individual's economic situation, health, personal
4	preferences, interests, reliability, behavior, location, or movements.
5	(44) "Protected health information" has the same meaning as in HIPAA.
6	(45) "Pseudonymous data" means personal data that cannot be attributed
7	to a specific individual without the use of additional information, provided the
8	additional information is kept separately and is subject to appropriate technical
9	and organizational measures to ensure that the personal data is not attributed to
10	an identified or identifiable individual.
11	(46)(A) "Publicly available information" means information that:
12	(i) is lawfully made available through federal, state, or local
13	government records; or
14	(ii) a controller has a reasonable basis to believe that the consumer
15	has lawfully made available to the general public through widely distributed
16	media.
17	(B) "Publicly available information" does not include biometric data
18	collected by a business about a consumer without the consumer's knowledge.
19	(47) "Qualified service organization" has the same meaning as in
20	42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

H.121 Page 13 of 98

1	(48) "Reproductive or sexual health care" has the same meaning as
2	"reproductive health care services" in 1 V.S.A. § 150(c)(1).
3	(49) "Reproductive or sexual health data" means any personal data
4	concerning a past, present, or future effort made by a consumer to seek, or a
5	consumer's receipt of, reproductive or sexual health care.
6	(50) "Reproductive or sexual health facility" means any health care
7	facility in which at least 70 percent of the health care-related services or
8	products rendered or provided in the facility are reproductive or sexual health
9	care.
10	(51)(A) "Sale of personal data" means the exchange of a consumer's
11	personal data by the controller to a third party for monetary or other valuable
12	consideration or otherwise for a commercial purpose.
13	(B) As used in this subdivision (51), "commercial purpose" means to
14	advance a person's commercial or economic interests, such as by inducing
15	another person to buy, rent, lease, join, subscribe to, provide, or exchange
16	products, goods, property, information, or services, or enabling or effecting,
17	directly or indirectly, a commercial transaction.
18	(C) "Sale of personal data" does not include:
19	(i) the disclosure of personal data to a processor that processes the
20	personal data on behalf of the controller;

H.121 Page 14 of 98

1	(ii) the disclosure of personal data to a third party for purposes of
2	providing a product or service requested by the consumer;
3	(iii) the disclosure or transfer of personal data to an affiliate of the
4	controller;
5	(iv) the disclosure of personal data where the consumer directs the
6	controller to disclose the personal data or intentionally uses the controller to
7	interact with a third party;
8	(v) the disclosure of personal data that the consumer:
9	(I) intentionally made available to the general public via a
10	channel of mass media; and
11	(II) did not restrict to a specific audience; or
12	(vi) the disclosure or transfer of personal data to a third party as an
13	asset that is part of a merger, acquisition, bankruptcy or other transaction, or a
14	proposed merger, acquisition, bankruptcy, or other transaction, in which the
15	third party assumes control of all or part of the controller's assets.
16	(52) "Sensitive data" means personal data that:
17	(A) reveals a consumer's government-issued identifier, such as a
18	Social Security number, passport number, state identification card, or driver's
19	license number, that is not required by law to be publicly displayed;

H.121 Page 15 of 98

1	(B) reveals a consumer's racial or ethnic origin, national origin,
2	citizenship or immigration status, religious or philosophical beliefs, or union
3	membership;
4	(C) reveals a consumer's sexual orientation, sex life, sexuality, or
5	status as transgender or nonbinary;
6	(D) reveals a consumer's status as a victim of a crime;
7	(E) is financial information, including a consumer's tax return and
8	account number, financial account log-in, financial account, debit card number
9	or credit card number in combination with any required security or access
10	code, password, or credentials allowing access to an account;
11	(F) is consumer health data;
12	(G) is personal data collected and analyzed concerning consumer
13	health data or personal data that describes or reveals a past, present, or future
14	mental or physical health condition, treatment, disability, or diagnosis,
15	including pregnancy, to the extent the personal data is not used by the
16	controller to identify a specific consumer's physical or mental health condition
17	or diagnosis;
18	(H) is biometric or genetic data;
19	(I) is personal data collected from a known minor; or
20	(J) is precise geolocation data.

	Η.	121
Page	16 of	f 98

1	(53)(A) "Targeted advertising" means the targeting of an advertisement
2	to a consumer based on the consumer's activity with one or more businesses,
3	distinctly branded websites, applications, or services, other than the controller,
4	distinctly branded website, application, or service with which the consumer is
5	intentionally interacting.
6	(B) "Targeted advertising" does not include:
7	(i) an advertisement based on activities within the controller's own
8	commonly branded website or online application;
9	(ii) an advertisement based on the context of a consumer's current
10	search query, visit to a website, or use of an online application;
11	(iii) an advertisement directed to a consumer in response to the
12	consumer's request for information or feedback; or
13	(iv) processing personal data solely to measure or report
14	advertising frequency, performance, or reach.
15	(54) "Third party" means a natural or legal person, public authority,
16	agency, or body, other than the consumer, controller, or processor or an
17	affiliate of the processor or the controller.
18	(55) "Trade secret" has the same meaning as in section 4601 of this title.
19	(56) "Victim services organization" means a nonprofit organization that
20	is established to provide services to victims or witnesses of child abuse,

19

(a) This chapter does not apply to:

H.121 Page 17 of 98

1	domestic violence, human trafficking, sexual assault, violent felony, or
2	stalking.
3	§ 2416. APPLICABILITY
4	(a) Except as provided in subsection (b) of this section, this chapter applies
5	to a person that conducts business in this State or a person that produces
6	products or services that are targeted to residents of this State and that during
7	the preceding calendar year:
8	(1) controlled or processed the personal data of not fewer than 25,000
9	consumers, excluding personal data controlled or processed solely for the
10	purpose of completing a payment transaction; or
11	(2) controlled or processed the personal data of not fewer than 12,500
12	consumers and derived more than 25 percent of the person's gross revenue
13	from the sale of personal data.
14	(b) Sections 2420, 2424, and 2428 of this title and the provisions of this
15	chapter concerning consumer health data and consumer health data controllers
16	apply to a person that conducts business in this State or a person that produces
17	products or services that are targeted to residents of this State.
18	§ 2417. EXEMPTIONS

H.121 Page 18 of 98

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	<u>Use;</u>
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

H.121 Page 19 of 98

l	(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;

H.121 Page 20 of 98

1	(9) information processed or maintained solely in connection with, and
2	for the purpose of, enabling:
3	(A) an individual's employment or application for employment;
4	(B) an individual's ownership of, or function as a director or officer
5	of, a business entity;
6	(C) an individual's contractual relationship with a business entity;
7	(D) an individual's receipt of benefits from an employer, including
8	benefits for the individual's dependents or beneficiaries; or
9	(E) notice of an emergency to persons that an individual specifies;
10	(10) any activity that involves collecting, maintaining, disclosing,
11	selling, communicating, or using information for the purpose of evaluating a
12	consumer's creditworthiness, credit standing, credit capacity, character,
13	general reputation, personal characteristics, or mode of living if done strictly in
14	accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C.
15	§ 1681–1681x, as may be amended, by:
16	(A) a consumer reporting agency;
17	(B) a person who furnishes information to a consumer reporting
18	agency under 15 U.S.C. § 1681s-2 (responsibilities of furnishers of
19	information to consumer reporting agencies); or

H.121 Page 21 of 98

1	(C) a person who uses a consumer report as provided in 15 U.S.C.
2	§ 1681b(a)(3) (permissible purposes of consumer reports);
3	(11) information collected, processed, sold, or disclosed under and in
4	accordance with the following laws and regulations:
5	(A) the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721–
6	<u>2725;</u>
7	(B) the Family Educational Rights and Privacy Act, 20 U.S.C.
8	§ 1232g, and regulations adopted to implement that act;
9	(C) the Airline Deregulation Act, Pub. L. No. 95-504, only to the
10	extent that an air carrier collects information related to prices, routes, or
11	services, and only to the extent that the provisions of the Airline Deregulation
12	Act preempt this chapter;
13	(D) the Farm Credit Act, Pub. L. No. 92-181, as may be amended;
14	(E) federal policy under 21 U.S.C. § 830 (regulation of listed
15	chemicals and certain machines);
16	(12) nonpublic personal information that is processed by a financial
17	institution subject to the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and
18	regulations adopted to implement that act;
19	(13) information that originates from, or is intermingled so as to be
20	indistinguishable from, information described in subdivision (12) of this

H.121 Page 22 of 98

1	subsection and that a controller or processor collects, processes, uses, or
2	maintains in the same manner as is required under the law and regulations
3	specified in subdivision (12) of this subsection;
4	(14) a financial institution, credit union, independent trust company,
5	broker-dealer, or investment adviser or a financial institution's, credit union's,
6	independent trust company's, broker-dealer's, or investment adviser's affiliate
7	or subsidiary that is only and directly engaged in financial activities, as
8	described in 12 U.S.C. § 1843(k);
9	(15) a person regulated pursuant to 8 V.S.A. part 3 (chapters 101–165)
10	other than a person that, alone or in combination with another person,
11	establishes and maintains a self-insurance program and that does not otherwise
12	engage in the business of entering into policies of insurance;
13	(16) a third-party administrator, as that term is defined in the Third Party
14	Administrator Rule adopted pursuant to 18 V.S.A. § 9417;
15	(17) personal data of a victim or witness of child abuse, domestic
16	violence, human trafficking, sexual assault, violent felony, or stalking that a
17	victim services organization collects, processes, or maintains in the course of
18	its operation;
19	(18) a nonprofit organization that is established to detect and prevent
20	fraudulent acts in connection with insurance;

H.121 Page 23 of 98

1	(19) information that is processed for purposes of compliance,
2	enrollment or degree verification, or research services by a nonprofit
3	organization that is established to provide enrollment data reporting services
4	on behalf of postsecondary schools as that term is defined in 16 V.S.A. § 176;
5	<u>or</u>
6	(20) noncommercial activity of:
7	(A) a publisher, editor, reporter, or other person who is connected
8	with or employed by a newspaper, magazine, periodical, newsletter, pamphlet,
9	report, or other publication in general circulation;
10	(B) a radio or television station that holds a license issued by the
11	Federal Communications Commission;
12	(C) a nonprofit organization that provides programming to radio or
13	television networks; or
14	(D) an entity that provides an information service, including a press
15	association or wire service.
16	(b) Controllers, processors, and consumer health data controllers that
17	comply with the verifiable parental consent requirements of COPPA shall be
18	deemed compliant with any obligation to obtain parental consent pursuant to
19	this chapter, including pursuant to section 2420 of this title.
20	§ 2418. CONSUMER PERSONAL DATA RIGHTS

H.121 Page 24 of 98

1	(a) A consumer shall have the right to:
2	(1) confirm whether a controller is processing the consumer's personal
3	data and, if a controller is processing the consumer's personal data, access the
4	personal data;
5	(2) obtain from a controller a list of third parties to which the controller
6	has disclosed the consumer's personal data or, if the controller does not
7	maintain this information in a format specific to the consumer, a list of third
8	parties to which the controller has disclosed personal data;
9	(3) correct inaccuracies in the consumer's personal data, taking into
10	account the nature of the personal data and the purposes of the processing of
11	the consumer's personal data;
12	(4) delete personal data provided by, or obtained about, the consumer
13	unless retention of the personal data is required by law;
14	(5) if the processing of personal data is done by automatic means, obtain
15	a copy of the consumer's personal data processed by the controller in a
16	portable and, to the extent technically feasible, readily usable format that
17	allows the consumer to transmit the data to another controller without
18	hindrance; and
19	(6) opt out of the processing of personal data for purposes of:
20	(A) targeted advertising;

1	(B) the sale of personal data; or
2	(C) profiling in furtherance of solely automated decisions that
3	produce legal or similarly significant effects concerning the consumer.
4	(b)(1) A consumer may exercise rights under this section by submitting a
5	request to a controller using the method that the controller specifies in the
6	privacy notice under section 2419 of this title.
7	(2) A controller shall not require a consumer to create an account for the
8	purpose described in subdivision (1) of this subsection, but the controller may
9	require the consumer to use an account the consumer previously created.
10	(3) A parent or legal guardian may exercise rights under this section on
11	behalf of the parent's child or on behalf of a child for whom the guardian has
12	legal responsibility. A guardian or conservator may exercise the rights under
13	this section on behalf of a consumer that is subject to a guardianship,
14	conservatorship, or other protective arrangement.
15	(4)(A) A consumer may designate another person to act on the
16	consumer's behalf as the consumer's authorized agent for the purpose of
17	exercising the consumer's rights under subdivision (a)(4) or (a)(6) of this
18	section.
19	(B) The consumer may designate an authorized agent by means of an
20	internet link, browser setting, browser extension, global device setting, or other

1	technology that enables the consumer to exercise the consumer's rights under
2	subdivision (a)(4) or (a)(6) of this section.
3	(c) Except as otherwise provided in this chapter, a controller shall comply
4	with a request by a consumer to exercise the consumer rights authorized
5	pursuant to this chapter as follows:
6	(1)(A) A controller shall respond to the consumer without undue delay,
7	but not later than 45 days after receipt of the request.
8	(B) The controller may extend the response period by 45 additional
9	days when reasonably necessary, considering the complexity and number of
10	the consumer's requests, provided the controller informs the consumer of the
11	extension within the initial 45-day response period and of the reason for the
12	extension.
13	(2) If a controller declines to take action regarding the consumer's
14	request, the controller shall inform the consumer without undue delay, but not
15	later than 45 days after receipt of the request, of the justification for declining
16	to take action and instructions for how to appeal the decision.
17	(3)(A) Information provided in response to a consumer request shall be
18	provided by a controller, free of charge, once per consumer during any 12-
19	month period.

1	(B) If requests from a consumer are manifestly unfounded, excessive
2	or repetitive, the controller may charge the consumer a reasonable fee to cover
3	the administrative costs of complying with the request or decline to act on the
4	request.
5	(C) The controller bears the burden of demonstrating the manifestly
6	unfounded, excessive, or repetitive nature of the request.
7	(4)(A) If a controller is unable to authenticate a request to exercise any
8	of the rights afforded under subdivisions (a)(1)–(5) of this section using
9	commercially reasonable efforts, the controller shall not be required to comply
10	with a request to initiate an action pursuant to this section and shall provide
11	notice to the consumer that the controller is unable to authenticate the request
12	to exercise the right or rights until the consumer provides additional
13	information reasonably necessary to authenticate the consumer and the
14	consumer's request to exercise the right or rights.
15	(B) A controller shall not be required to authenticate an opt-out
16	request, but a controller may deny an opt-out request if the controller has a
17	good faith, reasonable, and documented belief that the request is fraudulent.
18	(C) If a controller denies an opt-out request because the controller
19	believes the request is fraudulent, the controller shall send a notice to the
20	person who made the request disclosing that the controller believes the request

	ŀ	H.1	21
Page	28	of	98

1	is fraudulent, why the controller believes the request is fraudulent, and that the
2	controller shall not comply with the request.
3	(5) A controller that has obtained personal data about a consumer from a
4	source other than the consumer shall be deemed in compliance with a
5	consumer's request to delete the data pursuant to subdivision (a)(4) of this
6	section by:
7	(A) retaining a record of the deletion request and the minimum data
8	necessary for the purpose of ensuring the consumer's personal data remains
9	deleted from the controller's records and not using the retained data for any
10	other purpose pursuant to the provisions of this chapter; or
11	(B) opting the consumer out of the processing of the personal data for
12	any purpose except for those exempted pursuant to the provisions of this
13	chapter.
14	(6) A controller may not condition the exercise of a right under this
15	section through:
16	(A) the use of any false, fictitious, fraudulent, or materially
17	misleading statement or representation; or
18	(B) the employment of any dark pattern.

H.121 Page 29 of 98

1	(d) A controller shall establish a process by means of which a consumer
2	may appeal the controller's refusal to take action on a request under
3	subsection (b) of this section. The controller's process must:
4	(1) Allow a reasonable period of time after the consumer receives the
5	controller's refusal within which to appeal.
6	(2) Be conspicuously available to the consumer.
7	(3) Be similar to the manner in which a consumer must submit a request
8	under subsection (b) of this section.
9	(4) Require the controller to approve or deny the appeal within 45 days
10	after the date on which the controller received the appeal and to notify the
11	consumer in writing of the controller's decision and the reasons for the
12	decision. If the controller denies the appeal, the notice must provide or specify
13	information that enables the consumer to contact the Attorney General to
14	submit a complaint.
15	(e) Nothing in this section shall be construed to require a controller to
16	reveal a trade secret.
17	§ 2419. DUTIES OF CONTROLLERS
18	(a) A controller shall:

	ŀ	\mathbf{H} . 1	21
Page	30	of	98

1	(1) limit the collection of personal data to what is reasonably necessary
2	and proportionate to provide or maintain a specific product or service
3	requested by the consumer to whom the data pertains;
4	(2) establish, implement, and maintain reasonable administrative,
5	technical, and physical data security practices to protect the confidentiality,
6	integrity, and accessibility of personal data appropriate to the volume and
7	nature of the personal data at issue;
8	(3) provide an effective mechanism for a consumer to revoke consent to
9	the controller's processing of the consumer's personal data that is at least as
10	easy as the mechanism by which the consumer provided the consumer's
11	consent; and
12	(4) upon a consumer's revocation of consent to processing, cease to
13	process the consumer's personal data as soon as practicable, but not later than
14	15 days after receiving the request.
15	(b) A controller shall not:
16	(1) process personal data for a purpose not disclosed in the privacy
17	notice required under subsection (d) of this section unless:
18	(A) the controller obtains the consumer's consent; or
19	(B) the purpose is reasonably necessary to and compatible with a
20	disclosed purpose;

H.121 Page 31 of 98

1	(2) process sensitive data about a consumer without first obtaining the
2	consumer's consent or, if the controller knows the consumer is a child, without
3	processing the sensitive data in accordance with COPPA;
4	(3) sell sensitive data;
5	(4) discriminate or retaliate against a consumer who exercises a right
6	provided to the consumer under this chapter or refuses to consent to the
7	processing of personal data for a separate product or service, including by:
8	(A) denying goods or services;
9	(B) charging different prices or rates for goods or services; or
10	(C) providing a different level of quality or selection of goods or
11	services to the consumer;
12	(5) process personal data in violation of State or federal laws that
13	prohibit unlawful discrimination; or
14	(6)(A) except as provided in subdivision (B) of this subdivision (6),
15	process a consumer's personal data in a manner that discriminates against
16	individuals or otherwise makes unavailable the equal enjoyment of goods or
17	services on the basis of an individual's actual or perceived race, color, sex,
18	sexual orientation or gender identity, physical or mental disability, religion,
19	ancestry, or national origin;
20	(B) subdivision (A) of this subdivision (6) shall not apply to:

H.121 Page 32 of 98

1	(i) a private establishment, as that term is used in 42 U.S.C.
2	§ 2000a(e) (prohibition against discrimination or segregation in places of
3	public accommodation);
4	(ii) processing for the purpose of a controller's or processor's self-
5	testing to prevent or mitigate unlawful discrimination; or
6	(iii) processing for the purpose of diversifying an applicant,
7	participant, or consumer pool.
8	(c) Subsections (a) and (b) of this section shall not be construed to:
9	(1) require a controller to provide a good or service that requires
10	personal data from a consumer that the controller does not collect or maintain;
11	<u>or</u>
12	(2) prohibit a controller from offering a different price, rate, level of
13	quality, or selection of goods or services to a consumer, including an offer for
14	no fee or charge, in connection with a consumer's voluntary participation in a
15	financial incentive program, such as a bona fide loyalty, rewards, premium
16	features, discount, or club card program, provided that the controller may not
17	transfer personal data to a third party as part of the program unless:
18	(A) the transfer is necessary to enable the third party to provide a
19	benefit to which the consumer is entitled; or

]	H.12	1
Page	33	of 98	8

1	(B)(i) the terms of the program clearly disclose that personal data
2	will be transferred to the third party or to a category of third parties of which
3	the third party belongs; and
4	(ii) the consumer consents to the transfer.
5	(d)(1) A controller shall provide to consumers a reasonably accessible,
6	clear, and meaningful privacy notice that:
7	(A) lists the categories of personal data, including the categories of
8	sensitive data, that the controller processes;
9	(B) describes the controller's purposes for processing the personal
10	data;
11	(C) describes how a consumer may exercise the consumer's rights
12	under this chapter, including how a consumer may appeal a controller's denial
13	of a consumer's request under section 2418 of this title;
14	(D) lists all categories of personal data, including the categories of
15	sensitive data, that the controller shares with third parties;
16	(E) describes all categories of third parties with which the controller
17	shares personal data at a level of detail that enables the consumer to understand
18	what type of entity each third party is and, to the extent possible, how each
19	third party may process personal data;

H.121 Page 34 of 98

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.

H.121 Page 35 of 98

1	(e) The method or methods under subdivision (d)(1)(I) of this section for
2	submitting a consumer's request to a controller must:
3	(1) take into account the ways in which consumers normally interact
4	with the controller, the need for security and reliability in communications
5	related to the request, and the controller's ability to authenticate the identity of
6	the consumer that makes the request;
7	(2) provide a clear and conspicuous link to a website where the
8	consumer or an authorized agent may opt out from a controller's processing of
9	the consumer's personal data pursuant to subdivision 2418(a)(6) of this title or,
10	solely if the controller does not have a capacity needed for linking to a
11	webpage, provide another method the consumer can use to opt out; and
12	(3) allow a consumer or authorized agent to send a signal to the
13	controller that indicates the consumer's preference to opt out of the sale of
14	personal data or targeted advertising pursuant to subdivision 2418(a)(6) of this
15	title by means of a platform, technology, or mechanism that:
16	(A) does not unfairly disadvantage another controller;
17	(B) does not use a default setting but instead requires the consumer or
18	authorized agent to make an affirmative, voluntary, and unambiguous choice to
19	opt out;
20	(C) is consumer friendly and easy for an average consumer to use;

1	(D) is as consistent as possible with similar platforms, technologies,
2	or mechanisms required under federal or state laws or regulations; and
3	(E)(i) enables the controller to reasonably determine whether the
4	consumer has made a legitimate request pursuant to subsection 2418(b) of this
5	title to opt out pursuant to subdivision 2418(a)(6) of this title; and
6	(ii) for purposes of subdivision (i) of this subdivision (C), use of
7	an internet protocol address to estimate the consumer's location shall be
8	considered sufficient to accurately determine residency.
9	(f) If a consumer or authorized agent uses a method under subdivision
10	(d)(1)(I) of this section to opt out of a controller's processing of the
11	consumer's personal data pursuant to subdivision 2418(a)(6) of this title and
12	the decision conflicts with a consumer's voluntary participation in a bona fide
13	reward, club card, or loyalty program or a program that provides premium
14	features or discounts in return for the consumer's consent to the controller's
15	processing of the consumer's personal data, the controller may either comply
16	with the request to opt out or notify the consumer of the conflict and ask the
17	consumer to affirm that the consumer intends to withdraw from the bona fide
18	reward, club card, or loyalty program or the program that provides premium
19	features or discounts. If the consumer affirms that the consumer intends to
20	withdraw, the controller shall comply with the request to opt out.

8	§ 2420.	DUTIES	OF	CONTR	ROLLERS	TO	MINORS

^	() (1)		, 11	.1 .	CC		1.	•	1 4		C .	
,	(2)(1)	Δ	controller	that	offers	anv	Online	service -	nroduct	or	teature	$t \cap a$
_	(a)(1)	111		uiai	OHCIS	arry	Omme	SCI VICC,	product,	OI	icatuic	10 0

- 3 consumer whom the controller knows or consciously avoids knowing is a
- 4 minor shall use reasonable care to avoid any heightened risk of harm to minors
- 5 caused by the online service, product, or feature.
- 6 (2) In any action brought pursuant to section 2427 of this title, there is a
- 7 rebuttable presumption that a controller used reasonable care as required under
- 8 this section if the controller complied with this section.
- 9 (b) A controller that offers any online service, product, or feature to a
- 10 consumer whom the controller knows or consciously avoids knowing is a
- minor shall not process the minor's personal data for longer than is reasonably
- 12 necessary to provide the online service, product, or feature.
- 13 (c) A controller that offers any online service, product, or feature to a
- consumer whom the controller knows or consciously avoids knowing is a
- minor and who has consented under subdivision 2419(b)(2) of this title to the
- 16 processing of precise geolocation data shall:
- 17 (1) collect the minor's precise geolocation data only as reasonably
- 18 necessary for the controller to provide the online service, product, or feature;
- 19 and

1

H.121 Page 38 of 98

1	(2) provide to the minor a conspicuous signal indicating that the
2	controller is collecting the minor's precise geolocation data and make the
3	signal available to the minor for the entire duration of the collection of the
4	minor's precise geolocation data.
5	§ 2421. DUTIES OF PROCESSORS
6	(a) A processor shall adhere to a controller's instructions and shall assist
7	the controller in meeting the controller's obligations under this chapter. In
8	assisting the controller, the processor must:
9	(1) enable the controller to respond to requests from consumers pursuan
10	to subsection 2418(b) of this title by means that:
11	(A) take into account how the processor processes personal data and
12	the information available to the processor; and
13	(B) use appropriate technical and organizational measures to the
14	extent reasonably practicable;
15	(2) adopt administrative, technical, and physical safeguards that are
16	reasonably designed to protect the security and confidentiality of the personal
17	data the processor processes, taking into account how the processor processes
18	the personal data and the information available to the processor; and
19	(3) provide information reasonably necessary for the controller to
20	conduct and document data protection assessments.

	I	H.1	21
Page	39	of	98

1	(b) Processing by a processor must be governed by a contract between the
2	controller and the processor. The contract must:
3	(1) be valid and binding on both parties;
4	(2) set forth clear instructions for processing data, the nature and
5	purpose of the processing, the type of data that is subject to processing, and the
6	duration of the processing;
7	(3) specify the rights and obligations of both parties with respect to the
8	subject matter of the contract;
9	(4) ensure that each person that processes personal data is subject to a
10	duty of confidentiality with respect to the personal data;
11	(5) require the processor to delete the personal data or return the
12	personal data to the controller at the controller's direction or at the end of the
13	provision of services, unless a law requires the processor to retain the personal
14	data;
15	(6) require the processor to make available to the controller, at the
16	controller's request, all information the controller needs to verify that the
17	processor has complied with all obligations the processor has under this
18	chapter;
19	(7) require the processor to enter into a subcontract with a person the
20	processor engages to assist with processing personal data on the controller's

H.121 Page 40 of 98

1	behalf and in the subcontract require the subcontractor to meet the processor's
2	obligations concerning personal data;
3	(8)(A) allow the controller, the controller's designee, or a qualified and
4	independent person the processor engages, in accordance with an appropriate
5	and accepted control standard, framework, or procedure, to assess the
6	processor's policies and technical and organizational measures for complying
7	with the processor's obligations under this chapter;
8	(B) require the processor to cooperate with the assessment; and
9	(C) at the controller's request, report the results of the assessment to
10	the controller; and
11	(9) prohibit the processor from combining personal data obtained from
12	the controller with personal data that the processor:
13	(A) receives from or on behalf of another controller or person; or
14	(B) collects from an individual.
15	(c) This section does not relieve a controller or processor from any liability
16	that accrues under this chapter as a result of the controller's or processor's
17	actions in processing personal data.
18	(d)(1) For purposes of determining obligations under this chapter, a person
19	is a controller with respect to processing a set of personal data and is subject to

	J	H. J	121
Page	41	of	`98

1	an action under section 2427 of this title to punish a violation of this chapter, if
2	the person:
3	(A) does not adhere to a controller's instructions to process the
4	personal data; or
5	(B) begins at any point to determine the purposes and means for
6	processing the personal data, alone or in concert with another person.
7	(2) A determination under this subsection is a fact-based determination
8	that must take account of the context in which a set of personal data is
9	processed.
10	(3) A processor that adheres to a controller's instructions with respect to
11	a specific processing of personal data remains a processor.
12	§ 2422. DUTIES OF PROCESSORS TO MINORS
13	(a) A processor shall adhere to the instructions of a controller and shall:
14	(1) assist the controller in meeting the controller's obligations under
15	sections 2420 and 2424 of this title, taking into account:
16	(A) the nature of the processing;
17	(B) the information available to the processor by appropriate
18	technical and organizational measures; and
19	(C) whether the assistance is reasonably practicable and necessary to
20	assist the controller in meeting its obligations; and

H.121 Page 42 of 98

1	(2) provide any information that is necessary to enable the controller to
2	conduct and document data protection assessments pursuant to section 2424 of
3	this title.
4	(b) A contract between a controller and a processor must satisfy the
5	requirements in subsection 2421(b) of this title.
6	(c) Nothing in this section shall be construed to relieve a controller or
7	processor from the liabilities imposed on the controller or processor by virtue
8	of the controller's or processor's role in the processing relationship as
9	described in sections 2420 and 2424 of this title.
10	(d) Determining whether a person is acting as a controller or processor with
11	respect to a specific processing of data is a fact-based determination that
12	depends upon the context in which personal data is to be processed. A person
13	that is not limited in the person's processing of personal data pursuant to a
14	controller's instructions, or that fails to adhere to the instructions, is a
15	controller and not a processor with respect to a specific processing of data. A
16	processor that continues to adhere to a controller's instructions with respect to
17	a specific processing of personal data remains a processor. If a processor
18	begins, alone or jointly with others, determining the purposes and means of the
19	processing of personal data, the processor is a controller with respect to the

H.121 Page 43 of 98

1	processing and may be subject to an enforcement action under section 2427 of
2	this title.
3	§ 2423. DATA PROTECTION ASSESSMENTS FOR PROCESSING
4	ACTIVITIES THAT PRESENT A HEIGHTENED RISK OF HARM
5	TO A CONSUMER
6	(a) A controller shall conduct and document a data protection assessment
7	for each of the controller's processing activities that presents a heightened risk
8	of harm to a consumer, which, for the purposes of this section, includes:
9	(1) the processing of personal data for the purposes of targeted
10	advertising;
11	(2) the sale of personal data;
12	(3) the processing of personal data for the purposes of profiling, where
13	the profiling presents a reasonably foreseeable risk of:
14	(A) unfair or deceptive treatment of, or unlawful disparate impact on,
15	consumers;
16	(B) financial, physical, or reputational injury to consumers;
17	(C) a physical or other intrusion upon the solitude or seclusion, or the
18	private affairs or concerns, of consumers, where the intrusion would be
19	offensive to a reasonable person; or
20	(D) other substantial injury to consumers; and

H.121 Page 44 of 98

1	(4) the processing of sensitive data.
2	(b)(1) Data protection assessments conducted pursuant to subsection (a) of
3	this section shall:
4	(A) identify the categories of personal data processed, the purposes
5	for processing the personal data, and whether the personal data is being
6	transferred to third parties; and
7	(B) identify and weigh the benefits that may flow, directly and
8	indirectly, from the processing to the controller, the consumer, other
9	stakeholders, and the public against the potential risks to the consumer
10	associated with the processing, as mitigated by safeguards that can be
11	employed by the controller to reduce the risks.
12	(2) The controller shall factor into any data protection assessment the
13	use of de-identified data and the reasonable expectations of consumers, as well
14	as the context of the processing and the relationship between the controller and
15	the consumer whose personal data will be processed.
16	(c)(1) The Attorney General may require that a controller disclose any data
17	protection assessment that is relevant to an investigation conducted by the
18	Attorney General pursuant to section 2427 of this title, and the controller shall
19	make the data protection assessment available to the Attorney General.

	I	H. 1	21
Page	45	of	98

1	(2) The Attorney General may evaluate the data protection assessment
2	for compliance with the responsibilities set forth in this chapter.
3	(3) Data protection assessments shall be confidential and shall be
4	exempt from disclosure and copying under the Public Records Act.
5	(4) To the extent any information contained in a data protection
6	assessment disclosed to the Attorney General includes information subject to
7	attorney-client privilege or work product protection, the disclosure shall not
8	constitute a waiver of the privilege or protection.
9	(d) A single data protection assessment may address a comparable set of
10	processing operations that present a similar heightened risk of harm.
11	(e) If a controller conducts a data protection assessment for the purpose of
12	complying with another applicable law or regulation, the data protection
13	assessment shall be deemed to satisfy the requirements established in this
14	section if the data protection assessment is reasonably similar in scope and
15	effect to the data protection assessment that would otherwise be conducted
16	pursuant to this section.
17	(f) Data protection assessment requirements shall apply to processing
18	activities created or generated after July 1, 2025, and are not retroactive.
19	(g) A controller shall retain for at least five years all data protection
20	assessments the controller conducts under this section.

1	§ 2424. DATA PROTECTION ASSESSMENTS FOR ONLINE SERVICES,
2	PRODUCTS, OR FEATURES OFFERED TO MINORS
3	(a) A controller that offers any online service, product, or feature to a
4	consumer whom the controller knows or consciously avoids knowing is a
5	minor shall conduct a data protection assessment for the online service product
6	or feature:
7	(1) in a manner that is consistent with the requirements established in
8	section 2423 of this title; and
9	(2) that addresses:
10	(A) the purpose of the online service, product, or feature;
11	(B) the categories of a minor's personal data that the online service,
12	product, or feature processes;
13	(C) the purposes for which the controller processes a minor's
14	personal data with respect to the online service, product, or feature; and
15	(D) any heightened risk of harm to a minor that is a reasonably
16	foreseeable result of offering the online service, product, or feature to a minor.
17	(b) A controller that conducts a data protection assessment pursuant to
18	subsection (a) of this section shall review the data protection assessment as
19	necessary to account for any material change to the processing operations of

	I	H.1	21
Page	47	of	98

1	the online service, product, or leature that is the subject of the data protection
2	assessment.
3	(c) If a controller conducts a data protection assessment pursuant to
4	subsection (a) of this section or a data protection assessment review pursuant
5	to subsection (b) of this section and determines that the online service, product
6	or feature that is the subject of the assessment poses a heightened risk of harm
7	to a minor, the controller shall establish and implement a plan to mitigate or
8	eliminate the heightened risk.
9	(d)(1) The Attorney General may require that a controller disclose any data
10	protection assessment pursuant to subsection (a) of this section that is relevant
11	to an investigation conducted by the Attorney General pursuant to section 2427
12	of this title, and the controller shall make the data protection assessment
13	available to the Attorney General.
14	(2) The Attorney General may evaluate the data protection assessment
15	for compliance with the responsibilities set forth in this chapter.
16	(3) Data protection assessments shall be confidential and shall be
17	exempt from disclosure and copying under the Public Records Act.
18	(4) To the extent any information contained in a data protection
19	assessment disclosed to the Attorney General includes information subject to

H.121 Page 48 of 98

1	attorney-client privilege or work product protection, the disclosure shall not			
2	constitute a waiver of the privilege or protection.			
3	(e) A single data protection assessment may address a comparable set of			
4	processing operations that include similar activities.			
5	(f) If a controller conducts a data protection assessment for the purpose of			
6	complying with another applicable law or regulation, the data protection			
7	assessment shall be deemed to satisfy the requirements established in this			
8	section if the data protection assessment is reasonably similar in scope and			
9	effect to the data protection assessment that would otherwise be conducted			
10	pursuant to this section.			
11	(g) Data protection assessment requirements shall apply to processing			
12	activities created or generated after July 1, 2025, and are not retroactive.			
13	(h) A controller that conducts a data protection assessment pursuant to			
14	subsection (a) of this section shall maintain documentation concerning the data			
15	protection assessment for the longer of:			
16	(1) three years after the date on which the processing operations cease;			
17	<u>or</u>			
18	(2) the date the controller ceases offering the online service, product, or			
19	feature.			

H.121 Page 49 of 98

1	§ 2425. DE-IDENTIFIED OR PSEUDONYMOUS DATA		
2	(a) A controller in possession of de-identified data shall:		
3	(1) take reasonable measures to ensure that the data cannot be used to		
4	re-identify an identified or identifiable individual or be associated with an		
5	individual or device that identifies or is linked or reasonably linkable to an		
6	individual or household;		
7	(2) publicly commit to maintaining and using de-identified data without		
8	attempting to re-identify the data; and		
9	(3) contractually obligate any recipients of the de-identified data to		
10	comply with the provisions of this chapter.		
11	(b) This section does not prohibit a controller from attempting to re-		
12	identify de-identified data solely for the purpose of testing the controller's		
13	methods for de-identifying data.		
14	(c) This chapter shall not be construed to require a controller or processor		
15	<u>to:</u>		
16	(1) re-identify de-identified data; or		
17	(2) maintain data in identifiable form, or collect, obtain, retain, or access		
18	any data or technology, in order to associate a consumer with personal data in		
19	order to authenticate the consumer's request under subsection 2418(b) of this		
20	title; or		

H.121 Page 50 of 98

1	(3) comply with an authenticated consumer rights request if the
2	controller:
3	(A) is not reasonably capable of associating the request with the
4	personal data or it would be unreasonably burdensome for the controller to
5	associate the request with the personal data;
6	(B) does not use the personal data to recognize or respond to the
7	specific consumer who is the subject of the personal data or associate the
8	personal data with other personal data about the same specific consumer; and
9	(C) does not sell or otherwise voluntarily disclose the personal data
10	to any third party, except as otherwise permitted in this section.
11	(d) The rights afforded under subdivisions 2418(a)(1)–(5) of this title shall
12	not apply to pseudonymous data in cases where the controller is able to
13	demonstrate that any information necessary to identify the consumer is kept
14	separately and is subject to effective technical and organizational controls that
15	prevent the controller from accessing the information.
16	(e) A controller that discloses or transfers pseudonymous data or de-
17	identified data shall exercise reasonable oversight to monitor compliance with
18	any contractual commitments to which the pseudonymous data or de-identified
19	data is subject and shall take appropriate steps to address any breaches of those
20	contractual commitments

H.121 Page 51 of 98

1	§ 2426. CONSTRUCTION OF DUTIES OF CONTROLLERS AND
2	<u>PROCESSORS</u>
3	(a) This chapter shall not be construed to restrict a controller's, processor's
4	or consumer health data controller's ability to:
5	(1) comply with federal, state, or municipal laws, ordinances, or
6	regulations;
7	(2) comply with a civil, criminal, or regulatory inquiry, investigation,
8	subpoena, or summons by federal, state, municipal, or other governmental
9	authorities;
10	(3) cooperate with law enforcement agencies concerning conduct or
11	activity that the controller, processor, or consumer health data controller
12	reasonably and in good faith believes may violate federal, state, or municipal
13	laws, ordinances, or regulations;
14	(4) carry out obligations under a contract under subsection 2421(b) of
15	this title for a federal or State agency or local unit of government;
16	(5) investigate, establish, exercise, prepare for, or defend legal claims;
17	(6) provide a product or service specifically requested by the consumer
18	to whom the personal data pertains consistent with subdivision 2419(a)(1) of
19	this title;

H.121 Page 52 of 98

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:		

H.121 Page 53 of 98

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		

H.121 Page 54 of 98

1	consumer to a person covered by an evidentiary privilege under the laws of the
2	State as part of a privileged communication.
3	(3) Nothing in this chapter modifies 2020 Acts and Resolves No. 166,
4	Sec. 14 or authorizes the use of facial recognition technology by law
5	enforcement.
6	(d)(1) A controller, processor, or consumer health data controller that
7	discloses personal data to a processor or third-party controller pursuant to this
8	chapter shall not be deemed to have violated this chapter if the processor or
9	third-party controller that receives and processes the personal data violates this
10	chapter, provided, at the time the disclosing controller, processor, or consumer
11	health data controller disclosed the personal data, the disclosing controller,
12	processor, or consumer health data controller did not have actual knowledge
13	that the receiving processor or third-party controller would violate this chapter
14	(2) A third-party controller or processor receiving personal data from a
15	controller, processor, or consumer health data controller in compliance with
16	this chapter is not in violation of this chapter for the transgressions of the
17	controller, processor, or consumer health data controller from which the third-
18	party controller or processor receives the personal data.
19	(e) This chapter shall not be construed to:

	ŀ	1.1	21
Page	55	of	98

1	(1) impose any obligation on a controller, processor, or consumer health
2	data controller that adversely affects the rights or freedoms of any person,
3	including the rights of any person:
4	(A) to freedom of speech or freedom of the press guaranteed in the
5	First Amendment to the U.S. Constitution; or
6	(B) under 12 V.S.A. § 1615; or
7	(2) apply to any person's processing of personal data in the course of the
8	person's purely personal or household activities.
9	(f)(1) Personal data processed by a controller or consumer health data
10	controller pursuant to this section may be processed to the extent that the
11	processing is:
12	(A)(i) reasonably necessary and proportionate to the purposes listed
13	in this section; or
14	(ii) in the case of sensitive data, strictly necessary to the purposes
15	listed in this section; and
16	(B) adequate, relevant, and limited to what is necessary in relation to
17	the specific purposes listed in this section.
18	(2)(A) Personal data collected, used, or retained pursuant to subsection
19	(b) of this section shall, where applicable, take into account the nature and
20	purpose or purposes of the collection, use, or retention.

1	(B) Personal data collected, used, or retained pursuant to subsection
2	(b) of this section shall be subject to reasonable administrative, technical, and
3	physical measures to protect the confidentiality, integrity, and accessibility of
4	the personal data and to reduce reasonably foreseeable risks of harm to
5	consumers relating to the collection, use, or retention of personal data.
6	(g) If a controller or consumer health data controller processes personal
7	data pursuant to an exemption in this section, the controller or consumer health
8	data controller bears the burden of demonstrating that the processing qualifies
9	for the exemption and complies with the requirements in subsection (f) of this
10	section.
11	(h) Processing personal data for the purposes expressly identified in this
12	section shall not solely make a legal entity a controller or consumer health data
13	controller with respect to the processing.
14	(i) This chapter shall not be construed to require a controller, processor, or
15	consumer health data controller to implement an age-verification or age-gating
16	system or otherwise affirmatively collect the age of consumers. A controller,
17	processor, or consumer health data controller that chooses to conduct
18	commercially reasonable age estimation to determine which consumers are
19	minors is not liable for an erroneous age estimation.

H.121 Page 57 of 98

1	<u>§ 2427.</u>	ENFORCEMENT

2	(a) A person who violates this chapter or rules adopted pursuant to this
3	chapter commits an unfair and deceptive act in commerce in violation of
4	section 2453 of this title, and the Attorney General shall have exclusive
5	authority to enforce such violations except as provided in subsection (d) of this
6	section.
7	(b) The Attorney General has the same authority to adopt rules to
8	implement the provisions of this section and to conduct civil investigations,
9	enter into assurances of discontinuance, bring civil actions, and take other
10	enforcement actions as provided under chapter 63, subchapter 1 of this title.
11	(c)(1) If the Attorney General determines that a violation of this chapter or
12	rules adopted pursuant to this chapter may be cured, the Attorney General may,
13	prior to initiating any action for the violation, issue a notice of violation
14	extending a 60-day cure period to the controller, processor, or consumer health
15	data controller alleged to have violated this chapter or rules adopted pursuant
16	to this chapter.
17	(2) The Attorney General may, in determining whether to grant a
18	controller, processor, or consumer health data controller the opportunity to
19	cure an alleged violation described in subdivision (1) of this subsection,
20	consider:

H.121 Page 58 of 98

1	(A) the number of violations;
2	(B) the size and complexity of the controller, processor, or consumer
3	health data controller;
4	(C) the nature and extent of the controller's, processor's, or consumer
5	health data controller's processing activities;
6	(D) the substantial likelihood of injury to the public;
7	(E) the safety of persons or property;
8	(F) whether the alleged violation was likely caused by human or
9	technical error; and
10	(G) the sensitivity of the data.
11	(d)(1) The private right of action available to a consumer for violations of
12	this chapter or rules adopted pursuant to this chapter shall be exclusively as
13	provided under this subsection.
14	(2) A consumer who is harmed by a data broker's or large data holder's
15	violation of subdivision 2419(b)(2) of this title, subdivision 2419(b)(3) of this
16	title, or section 2428 of this title may bring an action under subsection 2461(b)
17	of this title for the violation, but the right available under subsection 2461(b) of
18	this title shall not be available for a violation of any other provision of this
19	chapter or rules adopted pursuant to this chapter.

H.121 Page 59 of 98

1	(e) 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;
7	(4) the number of actions brought under subsection (c) of this section;
8	(5) the proportion of actions brought under subsection (c) of this section
9	that proceed to trial;
10	(6) the data brokers or large data holders most frequently sued under
11	subsection (c) of this section; and
12	(7) any other matter the Attorney General deems relevant for the
13	purposes of the report.
14	§ 2428. CONFIDENTIALITY OF CONSUMER HEALTH DATA
15	Except as provided in subsections 2417(a) and (b) of this title and section
16	2426 of this title, no person shall:
17	(1) provide any employee or contractor with access to consumer health
18	data unless the employee or contractor is subject to a contractual or statutory
19	duty of confidentiality;

H.121 Page 60 of 98

1	(2) provide any processor with access to consumer health data unless the
2	person and processor comply with section 2421 of this title; or
3	(3) use a geofence to establish a virtual boundary that is within 1,850
4	feet of any health care facility, including any mental health facility or
5	reproductive or sexual health facility, for the purpose of identifying, tracking,
6	collecting data from, or sending any notification to a consumer regarding the
7	consumer's consumer health data.
8	Sec. 2. PUBLIC EDUCATION AND OUTREACH; ATTORNEY GENERAL
9	STUDY
10	(a) The Attorney General shall implement a comprehensive public
11	education, outreach, and assistance program for controllers and processors as
12	those terms are defined in 9 V.S.A. § 2415. The program shall focus on:
13	(1) the requirements and obligations of controllers and processors under
14	the Vermont Data Privacy Act;
15	(2) data protection assessments under 9 V.S.A. § 2421;
16	(3) enhanced protections that apply to children, minors, sensitive data,
17	or consumer health data as those terms are defined in 9 V.S.A. § 2415;
18	(4) a controller's obligations to law enforcement agencies and the
19	Attorney General's office;
20	(5) methods for conducting data inventories; and

]	H.1	21
Page	61	of	98

1	(6) any other matters the Attorney General deems appropriate.
2	(b) The Attorney General shall provide guidance to controllers for
3	establishing data privacy notices and opt-out mechanisms, which may be in the
4	form of templates.
5	(c) The Attorney General shall implement a comprehensive public
6	education, outreach, and assistance program for consumers as that term is
7	defined in 9 V.S.A. § 2415. The program shall focus on:
8	(1) the rights afforded consumers under the Vermont Data Privacy Act,
9	including:
10	(A) the methods available for exercising data privacy rights; and
11	(B) the opt-out mechanism available to consumers;
12	(2) the obligations controllers have to consumers;
13	(3) different treatment of children, minors, and other consumers under
14	the act, including the different consent mechanisms in place for children and
15	other consumers;
16	(4) understanding a privacy notice provided under the Act;
17	(5) the different enforcement mechanisms available under the Act,
18	including the consumer's private right of action; and
19	(6) any other matters the Attorney General deems appropriate.

1	(d) The Attorney General shall cooperate with states with comparable data
2	privacy regimes to develop any outreach, assistance, and education programs,
3	where appropriate.
4	(e) The Attorney General may have the assistance of the Vermont Law and
5	Graduate School in developing education, outreach, and assistance programs
6	under this section.
7	(f) On or before December 15, 2026, the Attorney General shall assess the
8	effectiveness of the implementation of the Act and submit a report to the
9	House Committee on Commerce and Economic Development and the Senate
10	Committee on Economic Development, Housing and General Affairs with its
11	findings and recommendations, including any proposed draft legislation to
12	address issues that have arisen since implementation.
13	Sec. 3. 9 V.S.A. chapter 62 is amended to read:
14	CHAPTER 62. PROTECTION OF PERSONAL INFORMATION
15	Subchapter 1. General Provisions
16	§ 2430. DEFINITIONS
17	As used in this chapter:
18	(1) "Biometric data" shall have the same meaning as in section 2415 of
19	this title.

1	(2)(A) "Brokered personal information" means one or more of the
2	following computerized data elements about a consumer, if categorized or
3	organized for dissemination to third parties:
4	(i) name;
5	(ii) address;
6	(iii) date of birth;
7	(iv) place of birth;
8	(v) mother's maiden name;
9	(vi) unique biometric data generated from measurements or
10	technical analysis of human body characteristics used by the owner or licensee
11	of the data to identify or authenticate the consumer, such as a fingerprint, retina
12	or iris image, or other unique physical representation or digital representation
13	of biometric data;
14	(vii) name or address of a member of the consumer's immediate
15	family or household;
16	(viii) Social Security number or other government-issued
17	identification number; or
18	(ix) other information that, alone or in combination with the other
19	information sold or licensed, would allow a reasonable person to identify the
20	consumer with reasonable certainty.

H.121 Page 64 of 98

1	(B) "Brokered personal information" does not include publicly
2	available information to the extent that it is related to a consumer's business or
3	profession.
4	(2)(3) "Business" means a controller, a consumer health data controller,
5	a processor, or a commercial entity, including a sole proprietorship,
6	partnership, corporation, association, limited liability company, or other group,
7	however organized and whether or not organized to operate at a profit,
8	including a financial institution organized, chartered, or holding a license or
9	authorization certificate under the laws of this State, any other state, the United
10	States, or any other country, or the parent, affiliate, or subsidiary of a financial
11	institution, but does not include the State, a State agency, any political
12	subdivision of the State, or a vendor acting solely on behalf of, and at the
13	direction of, the State.
14	(3)(4) "Consumer" means an individual residing in this State.
15	(5) "Consumer health data controller" has the same meaning as in
16	section 2415 of this title.
17	(6) "Controller" has the same meaning as in section 2415 of this title.
18	(4)(7)(A) "Data broker" means a business, or unit or units of a business,
19	separately or together, that knowingly collects and sells or licenses to third

H.121 Page 65 of 98

1	parties the brokered personal information of a consumer with whom the
2	business does not have a direct relationship.
3	(B) Examples of a direct relationship with a business include if the
4	consumer is a past or present:
5	(i) customer, client, subscriber, user, or registered user of the
6	business's goods or services;
7	(ii) employee, contractor, or agent of the business;
8	(iii) investor in the business; or
9	(iv) donor to the business.
10	(C) The following activities conducted by a business, and the
11	collection and sale or licensing of brokered personal information incidental to
12	conducting these activities, do not qualify the business as a data broker:
13	(i) developing or maintaining third-party e-commerce or
14	application platforms;
15	(ii) providing 411 directory assistance or directory information
16	services, including name, address, and telephone number, on behalf of or as a
17	function of a telecommunications carrier;
18	(iii) providing publicly available information related to a
19	consumer's business or profession; or

1	(iv) providing publicly available information via real-time or near-
2	real-time alert services for health or safety purposes.
3	(D) The phrase "sells or licenses" does not include:
4	(i) a one-time or occasional sale of assets of a business as part of a
5	transfer of control of those assets that is not part of the ordinary conduct of the
6	business; or
7	(ii) a sale or license of data that is merely incidental to the
8	business.
9	(5)(8)(A) "Data broker security breach" means an unauthorized
10	acquisition or a reasonable belief of an unauthorized acquisition of more than
11	one element of brokered personal information maintained by a data broker
12	when the brokered personal information is not encrypted, redacted, or
13	protected by another method that renders the information unreadable or
14	unusable by an unauthorized person.
15	(B) "Data broker security breach" does not include good faith but
16	unauthorized acquisition of brokered personal information by an employee or
17	agent of the data broker for a legitimate purpose of the data broker, provided
18	that the brokered personal information is not used for a purpose unrelated to
19	the data broker's business or subject to further unauthorized disclosure.

1	(C) In determining whether brokered personal information has been
2	acquired or is reasonably believed to have been acquired by a person without
3	valid authorization, a data broker may consider the following factors, among
4	others:
5	(i) indications that the brokered personal information is in the
6	physical possession and control of a person without valid authorization, such
7	as a lost or stolen computer or other device containing brokered personal
8	information;
9	(ii) indications that the brokered personal information has been
10	downloaded or copied;
11	(iii) indications that the brokered personal information was used
12	by an unauthorized person, such as fraudulent accounts opened or instances of
13	identity theft reported; or
14	(iv) that the brokered personal information has been made public.
15	(6)(9) "Data collector" means a person who, for any purpose, whether
16	by automated collection or otherwise, handles, collects, disseminates, or
17	otherwise deals with personally identifiable information, and includes the
18	State, State agencies, political subdivisions of the State, public and private
19	universities, privately and publicly held corporations, limited liability
20	companies, financial institutions, and retail operators.

H.121 Page 68 of 98

1	(7)(10) "Encryption" means use of an algorithmic process to transform
2	data into a form in which the data is rendered unreadable or unusable without
3	use of a confidential process or key.
4	(8)(11) "License" means a grant of access to, or distribution of, data by
5	one person to another in exchange for consideration. A use of data for the sole
6	benefit of the data provider, where the data provider maintains control over the
7	use of the data, is not a license.
8	(9)(12) "Login credentials" means a consumer's user name or e-mail
9	address, in combination with a password or an answer to a security question,
10	that together permit access to an online account.
11	(10)(13)(A) "Personally identifiable information" means a consumer's
12	first name or first initial and last name in combination with one or more of the
13	following digital data elements, when the data elements are not encrypted,
14	redacted, or protected by another method that renders them unreadable or
15	unusable by unauthorized persons:
16	(i) a Social Security number;
17	(ii) a driver license or nondriver State identification card number,
18	individual taxpayer identification number, passport number, military
19	identification card number, or other identification number that originates from

1	a government identification document that is commonly used to verify identity
2	for a commercial transaction;
3	(iii) a financial account number or credit or debit card number, if
4	the number could be used without additional identifying information, access
5	codes, or passwords;
6	(iv) a password, personal identification number, or other access
7	code for a financial account;
8	(v) unique biometric data generated from measurements or
9	technical analysis of human body characteristics used by the owner or licensee
10	of the data to identify or authenticate the consumer, such as a fingerprint, retina
11	or iris image, or other unique physical representation or digital representation
12	of biometric data;
13	(vi) genetic information; and
14	(vii)(I) health records or records of a wellness program or similar
15	program of health promotion or disease prevention;
16	(II) a health care professional's medical diagnosis or treatment
17	of the consumer; or
18	(III) a health insurance policy number.

1	(B) "Personally identifiable information" does not mean publicly
2	available information that is lawfully made available to the general public from
3	federal, State, or local government records.
4	(14) "Processor" has the same meaning as in section 2415 of this title.
5	(11)(15) "Record" means any material on which written, drawn, spoken,
6	visual, or electromagnetic information is recorded or preserved, regardless of
7	physical form or characteristics.
8	(12)(16) "Redaction" means the rendering of data so that the data are
9	unreadable or are truncated so that no not more than the last four digits of the
10	identification number are accessible as part of the data.
11	(13)(17)(A) "Security breach" means unauthorized acquisition of
12	electronic data, or a reasonable belief of an unauthorized acquisition of
13	electronic data, that compromises the security, confidentiality, or integrity of a
14	consumer's personally identifiable information or login credentials maintained
15	by a data collector.
16	(B) "Security breach" does not include good faith but unauthorized
17	acquisition of personally identifiable information or login credentials by an
18	employee or agent of the data collector for a legitimate purpose of the data
19	collector, provided that the personally identifiable information or login

H.121 Page 71 of 98

1	credentials are not used for a purpose unrelated to the data collector's business
2	or subject to further unauthorized disclosure.
3	(C) In determining whether personally identifiable information or
4	login credentials have been acquired or is reasonably believed to have been
5	acquired by a person without valid authorization, a data collector may consider
6	the following factors, among others:
7	(i) indications that the information is in the physical possession
8	and control of a person without valid authorization, such as a lost or stolen
9	computer or other device containing information;
10	(ii) indications that the information has been downloaded or
11	copied;
12	(iii) indications that the information was used by an unauthorized
13	person, such as fraudulent accounts opened or instances of identity theft
14	reported; or
15	(iv) that the information has been made public.
16	* * *
17	Subchapter 2. Security Breach Notice Act Data Security Breaches
18	* * *
19	§ 2436. NOTICE OF DATA BROKER SECURITY BREACH

H.121 Page 72 of 98

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

1	of the security breach or when the data broker provides notice to consumers
2	pursuant to this section, whichever is sooner.
3	(ii) If the date of the breach is unknown at the time notice is sent
4	to the Attorney General, the data broker shall send the Attorney General the
5	date of the breach as soon as it is known.
6	(iii) Unless otherwise ordered by a court of this State for good
7	cause shown, a notice provided under this subdivision (2)(A) shall not be
8	disclosed to any person other than the authorized agent or representative of the
9	Attorney General, a State's Attorney, or another law enforcement officer
10	engaged in legitimate law enforcement activities without the consent of the
11	data broker.
12	(B)(i) When the data broker provides notice of the breach pursuant to
13	subdivision (1) of this subsection (b), the data broker shall notify the Attorney
14	General of the number of Vermont consumers affected, if known to the data
15	broker, and shall provide a copy of the notice provided to consumers under
16	subdivision (1) of this subsection (b).
17	(ii) The data broker may send to the Attorney General a second
18	copy of the consumer notice, from which is redacted the type of brokered
19	personal information that was subject to the breach, that the Attorney General
20	shall use for any public disclosure of the breach

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

H.121 Page 75 of 98

1	security breach involving brokered personal information shall include a			
2	description of each of the following, if known to the data broker:			
3	(A) the incident in general terms;			
4	(B) the type of brokered personal information that was subject to the			
5	security breach;			
6	(C) the general acts of the data broker to protect the brokered			
7	personal information from further security breach;			
8	(D) a telephone number, toll-free if available, that the consumer may			
9	call for further information and assistance;			
10	(E) advice that directs the consumer to remain vigilant by reviewing			
11	account statements and monitoring free credit reports; and			
12	(F) the approximate date of the data broker security breach.			
13	(5) A data broker may provide notice of a security breach involving			
14	brokered personal information to a consumer by two or more of the following			
15	methods:			
16	(A) written notice mailed to the consumer's residence;			
17	(B) electronic notice, for those consumers for whom the data broker			
18	has a valid e-mail address, if:			
19	(i) the data broker's primary method of communication with the			
20	consumer is by electronic means, the electronic notice does not request or			

H.121 Page 76 of 98

1	contain a hypertext link to a request that the consumer provide personal			
2	information, and the electronic notice conspicuously warns consumers not to			
3	provide personal information in response to electronic communications			
4	regarding security breaches; or			
5	(ii) the notice is consistent with the provisions regarding electronic			
6	records and signatures for notices in 15 U.S.C. § 7001;			
7	(C) telephonic notice, provided that telephonic contact is made			
8	directly with each affected consumer and not through a prerecorded message;			
9	<u>or</u>			
10	(D) notice by publication in a newspaper of statewide circulation in			
11	the event the data broker cannot effectuate notice by any other means.			
12	(c) Exception.			
13	(1) Notice of a security breach pursuant to subsection (b) of this section			
14	is not required if the data broker establishes that misuse of brokered personal			
15	information is not reasonably possible and the data broker provides notice of			
16	the determination that the misuse of the brokered personal information is not			
17	reasonably possible pursuant to the requirements of this subsection. If the data			
18	broker establishes that misuse of the brokered personal information is not			
19	reasonably possible, the data broker shall provide notice of its determination			
20	that misuse of the brokered personal information is not reasonably possible and			

H.121 Page 77 of 98

1	a detailed explanation for said determination to the Vermont Attorney General.			
2	The data broker may designate its notice and detailed explanation to the			
3	Vermont Attorney General as a trade secret if the notice and detailed			
4	explanation meet the definition of trade secret contained in 1 V.S.A.			
5	§ 317(c)(9).			
6	(2) If a data broker established that misuse of brokered personal			
7	information was not reasonably possible under subdivision (1) of this			
8	subsection and subsequently obtains facts indicating that misuse of the			
9	brokered personal information has occurred or is occurring, the data broker			
10	shall provide notice of the security breach pursuant to subsection (b) of this			
11	section.			
12	(d) Waiver. Any waiver of the provisions of this subchapter is contrary to			
13	public policy and is void and unenforceable.			
14	(e) Enforcement.			
15	(1) With respect to a controller or processor other than a controller or			
16	processor licensed or registered with the Department of Financial Regulation			
17	under Title 8 or this title, the Attorney General and State's Attorney shall have			
18	sole and full authority to investigate potential violations of this chapter and to			
19	enforce, prosecute, obtain, and impose remedies for a violation of this chapter			
20	or any rules or regulations adopted pursuant to this chapter as the Attorney			

1	General and State's Attorney have under chapter 63 of this title. The Attorney
2	General may refer the matter to the State's Attorney in an appropriate case.
3	The Superior Courts shall have jurisdiction over any enforcement matter
4	brought by the Attorney General or a State's Attorney under this subsection.
5	(2) With respect to a controller or processor that is licensed or registered
6	with the Department of Financial Regulation under Title 8 or this title, the
7	Department of Financial Regulation shall have the full authority to investigate
8	potential violations of this chapter and to enforce, prosecute, obtain, and
9	impose remedies for a violation of this chapter or any rules or regulations
10	adopted pursuant to this chapter, as the Department has under Title 8 or this
11	title or any other applicable law or regulation.
12	* * *
13	Subchapter 5. Data Brokers
14	§ 2446. <u>DATA BROKERS;</u> ANNUAL REGISTRATION
15	(a) Annually, on or before January 31 following a year in which a person
16	meets the definition of data broker as provided in section 2430 of this title, a
17	data broker shall:
18	(1) register with the Secretary of State;
19	(2) pay a registration fee of \$100.00; and
20	(3) provide the following information:

1	(A) the name and primary physical, e-mail, and Internet internet
2	addresses of the data broker;
3	(B) if the data broker permits a consumer to opt out of the data
4	broker's collection of brokered personal information, opt out of its databases,
5	or opt out of certain sales of data:
6	(i) the method for requesting an opt-out;
7	(ii) if the opt-out applies to only certain activities or sales, which
8	ones; and
9	(iii) whether the data broker permits a consumer to authorize a
10	third party to perform the opt-out on the consumer's behalf;
11	(C) a statement specifying the data collection, databases, or sales
12	activities from which a consumer may not opt out;
13	(D) a statement whether the data broker implements a purchaser
14	credentialing process;
15	(E) the number of data broker security breaches that the data broker
16	has experienced during the prior year, and if known, the total number of
17	consumers affected by the breaches;
18	(F) where the data broker has actual knowledge that it possesses the
19	brokered personal information of minors, a separate statement detailing the

	ŀ	H.1	21
Page	80	of	98

1	data collection practices, databases, sales activities, and opt-out policies that
2	are applicable to the brokered personal information of minors; and
3	(G) any additional information or explanation the data broker
4	chooses to provide concerning its data collection practices.
5	(b) A data broker that fails to register pursuant to subsection (a) of this
6	section is liable to the State for:
7	(1) a civil penalty of \$50.00 \$125.00 for each day, not to exceed a total
8	of \$10,000.00 for each year, it fails to register pursuant to this section;
9	(2) an amount equal to the fees due under this section during the period
10	it failed to register pursuant to this section; and
11	(3) other penalties imposed by law.
12	(c) A data broker that omits required information from its registration shall
13	file an amendment to include the omitted information within 30 business days
14	following notification of the omission and is liable to the State for a civil
15	penalty of \$1,000.00 per day for each day thereafter.
16	(d) A data broker that files materially incorrect information in its
17	registration:
18	(1) is liable to the State for a civil penalty of \$25,000.00; and
19	(2) if it fails to correct the false information within 30 business days
20	after discovery or notification of the incorrect information, an additional civil

H.121 Page 81 of 98

1	penalty of \$1,000.00 per day for each day thereafter that it falls to correct the
2	information.
3	(e) The Attorney General may maintain an action in the Civil Division of
4	the Superior Court to collect the penalties imposed in this section and to seek
5	appropriate injunctive relief.
6	* * *
7	§ 2448. DATA BROKERS; CREDENTIALING
8	(a) Credentialing.
9	(1) A data broker shall maintain reasonable procedures designed to
10	ensure that the brokered personal information it discloses is used for a
11	legitimate and legal purpose.
12	(2) These procedures shall require that prospective users of the
13	information identify themselves, certify the purposes for which the information
14	is sought, and certify that the information shall be used for no other purpose.
15	(3) A data broker shall make a reasonable effort to verify the identity of
16	a new prospective user and the uses certified by the prospective user prior to
17	furnishing the user brokered personal information.
18	(4) A data broker shall not furnish brokered personal information to any
19	person if it has reasonable grounds for believing that the brokered personal
20	information will not be used for a legitimate and legal purpose.

H.121 Page 82 of 98

1	Sec. 4. STUDY; DATA BROKERS; OPT OUT
2	On or before January 1, 2025, the Secretary of State, in collaboration with
3	the Agency of Digital Services, the Attorney General, and interested parties,
4	shall review and report their findings and recommendations to the House
5	Committee on Commerce and Economic Development and the Senate
6	Committee on Economic Development, Housing and General Affairs
7	concerning one or more mechanisms for Vermont consumers to opt out of the
8	collection, retention, and sale of brokered personal information, including:
9	(1) an individual opt-out that requires a data broker to allow a consumer
10	to opt out of its data collection, retention, and sales practices through a reques
11	made directly to the data broker; and
12	(2) specifically considering the rules, procedures, and framework for
13	implementing the "accessible deletion mechanism" by the California Privacy
14	Protection Agency that takes effect on January 1, 2026, and approaches in
15	other jurisdictions if applicable:
16	(A) how to design and implement a State-facilitated general opt-out
17	mechanism;
18	(B) the associated implementation and operational costs;
19	(C) mitigation of security risks; and
20	(D) other relevant considerations.

- 1 Sec. 5. 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 $\frac{25,000}{1}$
- 7 12,500 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 $\frac{12,500}{1}$
- 10 $\underline{6,250}$ consumers and derived more than $\underline{25}$ $\underline{20}$ percent of the person's gross
- 11 revenue from the sale of personal data.
- 12 Sec. 6. 9 V.S.A. § 2416(a) is amended to read:
- 13 (a) Except as provided in subsection (b) of this section, this chapter applies
- to a person that conducts business in this State or a person that produces
- products or services that are targeted to residents of this State and that during
- 16 the preceding calendar year:
- 17 (1) controlled or processed the personal data of not fewer than $\frac{12,500}{1}$
- 18 <u>6,250</u> consumers, excluding personal data controlled or processed solely for
- 19 the purpose of completing a payment transaction; or

	ŀ	H.1	21
Page	84	of	98

1	(2) controlled or processed the personal data of not fewer than $6,250$
2	3,125 consumers and derived more than 20 percent of the person's gross
3	revenue from the sale of personal data.
4	Sec. 7. 9 V.S.A. chapter 62, subchapter 6 is added to read:
5	Subchapter 6. Age-Appropriate Design Code
6	§ 2449a. DEFINITIONS
7	As used in this subchapter:
8	(1)(A) "Affiliate" means a legal entity that shares common branding
9	with another legal entity or controls, is controlled by, or is under common
10	control with another legal entity.
11	(B) As used in subdivision (A) of this subdivision (1), "control" or
12	"controlled" means:
13	(i) ownership of, or the power to vote, more than 50 percent of the
14	outstanding shares of any class of voting security of a company;
15	(ii) control in any manner over the election of a majority of the
16	directors or of individuals exercising similar functions; or
17	(iii) the power to exercise controlling influence over the
18	management of a company.
19	(2) "Age-appropriate" means a recognition of the distinct needs and
20	diversities of minor consumers at different age ranges. In order to help support

	I	H. 1	21
Page	85	of	98

1	the design of online services, products, and features, covered businesses should
2	take into account the unique needs and diversities of different age ranges,
3	including the following developmental stages: zero to five years of age or
4	"preliterate and early literacy"; six to nine years of age or "core primary school
5	years"; 10 to 12 years of age or "transition years"; 13 to 15 years of age or
6	"early teens"; and 16 to 17 years or age or "approaching adulthood."
7	(3) "Age estimation" means a process that estimates that a user is likely
8	to be of a certain age, fall within an age range, or is over or under a certain age.
9	(A) Age estimation methods include:
10	(i) analysis of behavioral and environmental data the covered
11	business already collects about its users;
12	(ii) comparing the way a user interacts with a device or with users
13	of the same age;
14	(iii) metrics derived from motion analysis; and
15	(iv) testing a user's capacity or knowledge.
16	(B) Age estimation does not require certainty, and if a covered
17	business estimates a user's age for the purpose of advertising or marketing, that
18	estimation may also be used to comply with this act.

1	(4) "Age verification" means a system that relies on hard identifiers or
2	verified sources of identification to confirm a user has reached a certain age,
3	including government-issued identification or a credit card.
4	(5) "Business associate" has the same meaning as in HIPAA.
5	(6) "Collect" means buying, renting, gathering, obtaining, receiving, or
6	accessing any personal data by any means. This includes receiving data from
7	the consumer, either actively or passively, or by observing the consumer's
8	behavior.
9	(7)(A) "Consumer" means an individual who is a resident of the State.
10	(B) "Consumer" does not include an individual acting in a
11	commercial or employment context or as an employee, owner, director, officer,
12	or contractor of a company, partnership, sole proprietorship, nonprofit, or
13	government agency whose communications or transactions with the covered
14	business occur solely within the context of that individual's role with the
15	company, partnership, sole proprietorship, nonprofit, or government agency.
16	(8) "Covered business" means a sole proprietorship, partnership, limited
17	liability company, corporation, association, other legal entity, or an affiliate
18	thereof, that conducts business in this State or that produces online products,
19	services, or features that are targeted to residents of this State and that:

H.121 Page 87 of 98

1	(A) collects consumers' personal data or has consumers' personal
2	data collected on its behalf by a third party;
3	(B) alone or jointly with others determines the purposes and means of
4	the processing of consumers personal data; and
5	(C) alone or in combination annually buys, receives for commercial
6	purposes, sells, or shares for commercial purposes, alone or in combination,
7	the personal data of at least 50 percent of its consumers.
8	(9) "Covered entity" has the same meaning as in HIPAA.
9	(10) "Dark pattern" means a user interface designed or manipulated with
10	the substantial effect of subverting or impairing user autonomy, decision
11	making, or choice, and includes any practice the Federal Trade Commission
12	refers to as a "dark pattern."
13	(11) "Default" means a preselected option adopted by the covered
14	business for the online service, product, or feature.
15	(12) "De-identified data" means data that does not identify and cannot
16	reasonably be used to infer information about, or otherwise be linked to, an
17	identified or identifiable individual, or a device linked to the individual, if the
18	covered business that possesses the data:
19	(A)(i) takes reasonable measures to ensure that the data cannot be
20	used to re-identify an identified or identifiable individual or be associated with

H.121 Page 88 of 98

1	an individual or device that identifies or is linked or reasonably linkable to an
2	individual or household;
3	(ii) for purposes of this subdivision (A), "reasonable measures"
4	shall include the de-identification requirements set forth under 45 C.F.R.
5	§ 164.514 (other requirements relating to uses and disclosures of protected
6	health information);
7	(B) publicly commits to process the data only in a deidentified
8	fashion and not attempt to re-identify the data; and
9	(C) contractually obligates any recipients of the data to comply with
10	all provisions of this subchapter.
11	(13) "Derived data" means data that is created by the derivation of
12	information, data, assumptions, correlations, inferences, predictions, or
13	conclusions from facts, evidence, or another source of information or data
14	about a minor consumer or a minor consumer's device.
15	(14) "Identified or identifiable individual" means an individual who can
16	be readily identified, directly or indirectly, including by reference to an
17	identifier such as a name, an identification number, specific geolocation data,
18	or an online identifier.

1	(15)(A) "Low-friction variable reward" means a design feature or
2	virtual item that intermittently rewards consumers for scrolling, tapping,
3	opening, or continuing to engage in an online service, product, or feature.
4	(B) Examples of low-friction variable reward designs include
5	endless scroll, auto play, and nudges meant to encourage reengagement.
6	(16)(A) "Minor consumer" means an individual under 18 years of age
7	who is a resident of the State.
8	(B) "Minor consumer" does not include an individual acting in a
9	commercial or employment context or as an employee, owner, director, officer,
10	or contractor of a company, partnership, sole proprietorship, nonprofit, or
11	government agency whose communications or transactions with the controller
12	occur solely within the context of that individual's role with the company,
13	partnership, sole proprietorship, nonprofit, or government agency.
14	(17) "Online service, product, or feature" means a digital product that is
15	accessible to the public via the internet, including a website or application, and
16	does not mean any of the following:
17	(A) telecommunications service, as defined in 47 U.S.C. § 153;
18	(B) a broadband internet access service as defined in 47 C.F.R.
19	§ 54.400; or
20	(C) the sale, delivery, or use of a physical product.

H.121 Page 90 of 98

1	(18)(A) "Personal data" means any information, including derived data
2	and unique identifiers, that is linked or reasonably linkable to an identified or
3	identifiable individual or to a device that identifies, is linked to, or is
4	reasonably linkable to one or more identified or identifiable individuals in a
5	household.
6	(B) Personal data does not include de-identified data or publicly
7	available information.
8	(19) "Process" or "processing" means any operation or set of operations
9	performed, whether by manual or automated means, on personal data or on sets
10	of personal data, such as the collection, use, storage, disclosure, analysis,
11	deletion, modification, or otherwise handling of personal data.
12	(20) "Processor" means a person who processes personal data on behalf
13	of a covered business.
14	(21) "Profiling" means any form of automated processing performed on
15	personal data to evaluate, analyze, or predict personal aspects related to an
16	identified or identifiable individual's economic situation, health, personal
17	preferences, interests, reliability, behavior, location, or movements.
18	(22) "Publicly available information" means information that:
19	(A) is lawfully made available through federal, state, or local
20	government records; or

1	(B) a covered business has a reasonable basis to believe that the
2	minor consumer has lawfully made available to the general public through
3	widely distributed media.
4	(23) "Reasonably likely to be accessed" means an online service,
5	product, or feature that is likely to be accessed by minor consumers based on
6	any of the following indicators:
7	(A) the online service, product, or feature is directed to children, as
8	defined by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-
9	6506 and the Federal Trade Commission rules implementing that Act;
10	(B) the online service, product, or feature is determined, based on
11	competent and reliable evidence regarding audience composition, to be
12	routinely accessed by an audience that is composed of at least two percent
13	minor consumers two through under 18 years of age;
14	(C) the online service, product, or feature contains advertisements
15	marketed to minor consumers;
16	(D) the audience of the online service, product, or feature is
17	determined, based on internal company research, to be composed of at least
18	two percent minor consumers two through under 18 years of age; or
19	(E) the covered business knew or should have known that at least two
20	percent of the audience of the online service, product, or feature includes

	ŀ	1.1	21
Page	92	of	98

1	minor consumers two through under 18 years of age, provided that, in making
2	this assessment, the business shall not collect or process any personal data that
3	is not reasonably necessary to provide an online service, product, or feature
4	with which a minor consumer is actively and knowingly engaged.
5	(24)(A) "Social media platform" means a public or semi-public internet-
6	based service or application that is primarily intended to connect and allow a
7	user to socially interact within such service or application and enables a user
8	<u>to:</u>
9	(i) construct a public or semi-public profile for the purposes of
10	signing into and using such service or application;
11	(ii) populate a public list of other users with whom the user shares
12	a social connection within such service or application; or
13	(iii) create or post content that is viewable by other users,
14	including content on message boards and in chat rooms, and that presents the
15	user with content generated by other users.
16	(B) "Social media platform" does not mean a public or semi-public
17	internet-based service or application that:
18	(i) exclusively provides electronic mail or direct messaging
19	services;

H.121 Page 93 of 98

1	(ii) primarily consists of news, sports, entertainment, interactive
2	video games, electronic commerce, or content that is preselected by the
3	provider for which any interactive functionality is incidental to, directly related
4	to, or dependent on the provision of such content; or
5	(iii) is used by and under the direction of an educational entity,
6	including a learning management system or a student engagement program.
7	(25) "Third party" means a natural or legal person, public authority,
8	agency, or body other than the minor consumer or the covered business.
9	§ 2449b. EXCLUSIONS
10	This subchapter does not apply to:
11	(1) a federal, state, tribal, or local government entity in the ordinary
12	course of its operation;
13	(2) protected health information that a covered entity or business
14	associate processes in accordance with, or documents that a covered entity or
15	business associate creates for the purpose of complying with, HIPAA;
16	(3) information used only for public health activities and purposes
17	described in 45 C.F.R. § 164.512;
18	(4) information that identifies a consumer in connection with:
19	(A) activities that are subject to the Federal Policy for the Protection
20	of Human Subjects as set forth in 45 C.F.R. Part 46;

H.121 Page 94 of 98

1	(B) research on human subjects undertaken in accordance with good
2	clinical practice guidelines issued by the International Council for
3	Harmonisation of Technical Requirements for Pharmaceuticals for Human
4	<u>Use;</u>
5	(C) activities that are subject to the protections provided in 21 C.F.R.
6	Part 50 and 21 C.F.R. Part 56; or
7	(D) research conducted in accordance with the requirements set forth
8	in subdivisions (A)–(C) of this subdivision (4) or otherwise in accordance with
9	State or federal law; and
10	(5) an entity whose primary purpose is journalism as defined in
11	12 V.S.A. § 1615(a)(2) and that has a majority of its workforce consisting of
12	individuals engaging in journalism.
13	§ 2449c. MINIMUM DUTY OF CARE
14	(a) A covered business that processes a minor consumer's data in any
15	capacity owes a minimum duty of care to the minor consumer.
16	(b) As used in this subchapter, "a minimum duty of care" means the use of
17	the personal data of a minor consumer and the design of an online service,
18	product, or feature will not benefit the covered business to the detriment of a
19	minor consumer and will not result in:

	ŀ	H.1	21
Page	95	of	98

1	(1) reasonably foreseeable emotional distress as defined in 13 V.S.A.		
2	§ 1061(2) to a minor consumer;		
3	(2) the encouragement of excessive or compulsive use of the online		
4	service, product, or feature by a minor consumer; or		
5	(3) discrimination against the minor consumer based upon race,		
6	ethnicity, sex, disability, sexual orientation, gender identity, gender expression,		
7	or national origin.		
8	§ 2449d. COVERED BUSINESS OBLIGATIONS		
9	(a) A covered business that is reasonably likely to be accessed and subject		
10	to this subchapter shall:		
11	(1) configure all default privacy settings provided to a minor consumer		
12	through the online service, product, or feature to a high level of privacy;		
13	(2) provide privacy information, terms of service, policies, and		
14	community standards concisely and prominently;		
15	(3) provide prominent, accessible, and responsive tools to help a minor		
16	consumer or, if applicable, their parents or guardians to exercise their privacy		
17	rights and report concerns to the covered business;		
18	(4) honor the request of a minor consumer to unpublish the minor		
19	consumer's social media platform account not later than 15 business days after		
20	a covered business receives such a request from a minor consumer; and		

H.121 Page 96 of 98

1	(5) provide easily accessible and age-appropriate tools for a minor		
2	consumer to limit the ability of users or covered businesses to send unsolicited		
3	communications.		
4	(b) A violation of this section constitutes a violation of the minimum duty		
5	of care as provided in section 2449c of this subchapter.		
6	§ 2449e. COVERED BUSINESS PROHIBITIONS		
7	(a) A covered business that is reasonably likely to be accessed and subject		
8	to this subchapter shall not:		
9	(1) use low-friction variable reward design features that encourage		
10	excessive and compulsive use by a minor consumer;		
11	(2) permit, by default, an unknown adult to contact a minor consumer on		
12	its platform without the minor consumer first initiating that contact;		
13	(3) permit a minor consumer to be exploited by a contract on the online		
14	service, product, or feature;		
15	(4) use dark patterns; or		
16	(5) permit a parent or guardian of a minor consumer, or any other		
17	consumer, to monitor the online activity of a minor consumer or to track the		
18	location of the minor consumer without providing a conspicuous signal to the		
19	minor consumer when the minor consumer is being monitored or tracked.		

1

	•
2	of care as provided in section 2449c of this subchapter.
3	§ 2449f. ATTORNEY GENERAL ENFORCEMENT
4	(a) A covered business that violates this subchapter or rules adopted
5	pursuant to this subchapter commits an unfair and deceptive act in
6	commerce in violation of section 2453 of this title.
7	(b) The Attorney General shall have the same authority under this
8	subchapter to make rules, conduct civil investigations, bring civil actions,
9	and enter into assurances of discontinuance as provided under chapter 63 of
10	this title.
11	§ 2449g. LIMITATIONS
12	Nothing in this subchapter shall be interpreted or construed to:
13	(1) Impose liability in a manner that is inconsistent with 47 U.S.C.
14	<u>§ 230.</u>
15	(2) Prevent or preclude any minor consumer from deliberately or
16	independently searching for, or specifically requesting, content.
17	(3) Require a covered business to implement an age verification
18	requirement. The obligations imposed under this act should be done with age
19	estimation techniques and do not require age verification.

(b) A violation of this section constitutes a violation of the minimum duty

1	8 2440h	RIGHTS	۸ND	FREEDOMS	OF MINOR	CONSUMER
1	0 Z449n.	KIGHIS	AND	LKEEDOM2	OF MINOR	CONSUMER

- 2 It is the intent of the General Assembly that nothing in this act may be
- 3 construed to infringe on the existing rights and freedoms of minor consumers
- 4 or be construed to discriminate against the minor consumer based on race,
- 5 ethnicity, sex, disability, sexual orientation, gender identity, gender expression,
- 6 or national origin.
- 7 Sec. 8. EFFECTIVE DATES
- 8 (a) This section and Secs. 2 (public education and outreach), 3 (protection
- 9 of personal information), and 4 (data broker opt-out study) shall take effect on
- 10 July 1, 2024.
- 11 (b) Secs. 1 (Vermont Data Privacy Act) and 7 (Age-Appropriate Design
- 12 Code) shall take effect on July 1, 2025.
- 13 (c) Sec. 5 (Vermont Data Privacy Act middle applicability threshold) shall
- take effect on July 1, 2026.
- 15 (d) Sec. 6 (Vermont Data Privacy Act low applicability threshold) shall
- take effect on July 1, 2027.
- and that after passage the title of the bill be amended to read: "An act
- relating to enhancing consumer privacy and the age-appropriate design code"