

**Senate proposal of amendment to House proposal of amendment to
Senate proposal of Amendment**

H.121.

An act relating to enhancing consumer privacy

The Senate concurs in the House proposal of amendment to Senate proposal of amendment with the following further proposals of amendment thereto:

First: In Sec. 1, 9 V.S.A. chapter 61A, by striking out section 2415 in its entirety and inserting in lieu thereof a new section 2415 to read as follows:

§ 2415. DEFINITIONS

As used in this chapter:

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

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

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

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

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

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

(A) Age estimation methods include:

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

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

(iii) metrics derived from motion analysis; and

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

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

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

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

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

(i) iris or retina scans;

(ii) fingerprints;

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

(iv) vein patterns;

(v) voice prints; and

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

(B) “Biometric data” does not include:

(i) a digital or physical photograph;

(ii) an audio or video recording; or

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

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

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

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

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

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

(C) “Consent” does not include:

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

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

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

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

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

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

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

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

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

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

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

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

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

(19) “Data broker” has the same meaning as in section 2430 of this title.

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

(21) “De-identified data” means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an

identified or identifiable individual, or a device linked to the individual, if the controller that possesses the data:

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

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

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

(C) contractually obligates any recipients of the data to satisfy the criteria set forth in subdivisions (A) and (B) of this subdivision (21).

(22) “Financial institution”:

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

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

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

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

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

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

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

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

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

(27) “Health care component” has the same meaning as in HIPAA.

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

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

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

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

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

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

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

(31) “Hybrid entity” has the same meaning as in HIPAA.

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

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

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

(35) “Large data holder” means a person that during the preceding calendar year processed the personal data of not fewer than 100,000 consumers.

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

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

(38)(A) “Online service, product, or feature” means any service, product, or feature that is provided online, except as provided in subdivision (B) of this subdivision (38).

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

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

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

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

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

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

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

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

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

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

(i) the content of communications;

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

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

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

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

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

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

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

(48)(A) “Publicly available information” means information that:

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

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

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

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

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

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

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

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

(B) As used in this subdivision (53), “commercial purpose” means to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

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

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

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

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

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

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

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

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

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

(54) "Sensitive data" means personal data that:

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

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

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

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

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

(F) is consumer health data;

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

(H) is biometric or genetic data;

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

(J) is precise geolocation data.

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

(B) “Targeted advertising” does not include:

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

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

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

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

(56) “Third party” means a natural or legal person, public authority, agency, or body, other than the consumer, controller, or processor or an affiliate of the processor or the controller.

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

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

Second: In Sec. 1, 9 V.S.A. chapter 61A, by striking out subsection 2417(a) in its entirety and inserting in lieu thereof a new subsection 2417(a) to read as follows:

(a) This chapter does not apply to:

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

(2) a covered entity that is not a hybrid entity, any health care component of a hybrid entity, or a business associate;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(10) any activity that involves collecting, maintaining, disclosing, selling, communicating, or using information for the purpose of evaluating a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living if done strictly in accordance with the

provisions of the Fair Credit Reporting Act, 15 U.S.C. § 1681–1681x, as may be amended, by:

(A) a consumer reporting agency;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(20) noncommercial activity of:

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

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

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

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

(21) a public utility subject to the jurisdiction of the Public Utility Commission under 30 V.S.A. § 203, but only until July 1, 2026.

Third: In Sec. 1, 9 V.S.A. chapter 61A, by striking out section 2427 in its entirety and inserting in lieu thereof a new section 2427 to read as follows:

§ 2427. ENFORCEMENT; ATTORNEY GENERAL'S POWERS

(a) A person who violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title, provided that a private right of action under subsection 2461(b) of this title shall not apply to the violation, and the Attorney General shall have exclusive authority to enforce such violations.

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

(c)(1) If the Attorney General determines that a violation of this chapter or rules adopted pursuant to this chapter may be cured, the Attorney General may,

prior to initiating any action for the violation, issue a notice of violation extending a 60-day cure period to the controller, processor, or consumer health data controller alleged to have violated this chapter or rules adopted pursuant to this chapter.

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

(A) the number of violations;

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

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

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

(E) the safety of persons or property;

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

(G) the sensitivity of the data.

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

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

(2) the nature of each violation;

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

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

Fourth: In Sec. 7, 9 V.S.A. chapter 62, subchapter 6, in subdivision 2449a(10), following “designed or manipulated with the”, by striking out the word “substantial”

Fifth: By striking out Sec. 8, effective dates, in its entirety and inserting in lieu thereof five new sections to be Secs. 8–12 to read as follows:

Sec. 8. STUDY; VERMONT DATA PRIVACY ACT

On or before January 15, 2026, the Attorney General shall review and report their findings and recommendations to the House Committees on Commerce and Economic Development, on Health Care, and on Judiciary and the Senate Committees on Economic Development, Housing and General Affairs, on

Health and Welfare, and on Judiciary concerning policy recommendations for improving data privacy in Vermont through:

(1) development of legislative language for implementing a private right of action in 9 V.S.A. chapter 61A, giving consideration to other state approaches and including through structuring:

(A) violations giving rise to a private right of action in a manner that addresses the gravest harms to consumers;

(B) applicability thresholds to ensure that the private right of action does not harm good-faith actors or small Vermont businesses;

(C) damages that balance the consumer interest in enforcing the consumer's personal data rights against the incentives a private right of action may provide to litigants with frivolous claims; and

(D) other mechanisms to ensure the private right of action is targeted to address persons engaging in unfair or deceptive acts;

(2) addressing the scope of health care exemptions under 9 V.S.A. § 2417(a)(2)–(8), including based on:

(I) research on the effects on the health care industry of the health-related data-level exemptions under the Oregon Consumer Privacy Act;

(II) economic analysis of compliance costs for the health care industry; and

(III) an analysis of health-related entities excluded from the health care exemptions under 9 V.S.A. § 2417(a)(2)–(8); and

(3) analysis of the data security implications of implementation of the Vermont Data Privacy Act.

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

§ 2427. ENFORCEMENT; ATTORNEY GENERAL'S POWERS

(a) A person who violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title, ~~provided that a consumer private right of action under subsection 2461(b) of this title shall not apply to the violation,~~ and the Attorney General shall have exclusive authority to enforce such violations except as provided in subsection (d) of this section.

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

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

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

(A) the number of violations;

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

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

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

(E) the safety of persons or property;

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

(G) the sensitivity of the data.

(d)(1) The private right of action available to a consumer for violations of this chapter or rules adopted pursuant to this chapter shall be exclusively as provided under this subsection.

(2) A consumer who is harmed by a data broker's or large data holder's violation of subdivision 2419(b)(2) of this title, subdivision 2419(b)(3) of this title, or section 2428 of this title may bring an action under subsection 2461(b) of this title for the violation, but the right available under subsection 2461(b) of this title shall not be available for a violation of any other provision of this chapter or rules adopted pursuant to this chapter.

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

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

(2) the nature of each violation;

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

(4) the number of actions brought under subsection (d) of this section;

(5) the proportion of actions brought under subsection (d) of this section that proceed to trial;

(6) the data brokers or large data holders most frequently sued under subsection (d) of this section; and

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

Sec. 10. 9 V.S.A. § 2427 is amended to read:

§ 2427. ENFORCEMENT; ATTORNEY GENERAL'S POWERS

(a) A person who violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title, provided that a consumer private right of action under subsection 2461(b) of this title shall not apply to the violation, and the Attorney General shall have exclusive authority to enforce such violations ~~except as provided in subsection (d) of this section~~.

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

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

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

(A) the number of violations;

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

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

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

(E) the safety of persons or property;

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

(G) the sensitivity of the data.

~~(d)(1) The private right of action available to a consumer for violations of this chapter or rules adopted pursuant to this chapter shall be exclusively as provided under this subsection.~~

~~(2) A consumer who is harmed by a data broker's or large data holder's violation of subdivision 2419(b)(2) of this title, subdivision 2419(b)(3) of this title, or section 2428 of this title may bring an action under subsection 2461(b) of this title for the violation, but the right available under subsection 2461(b) of this title shall not be available for a violation of any other provision of this chapter or rules adopted pursuant to this chapter.~~

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

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

(2) the nature of each violation;

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

~~(4) the number of actions brought under subsection (d) of this section;~~

~~(5) the proportion of actions brought under subsection (d) of this section that proceed to trial;~~

~~(6) the data brokers or large data holders most frequently sued under subsection (d) of this section; and~~

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

Sec. 11. 9 V.S.A. § 2417(a) is amended to read:

(a) This chapter does not apply to:

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

(2) a covered entity that is not a hybrid entity, any health care component of a hybrid entity, or a business associate;

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

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

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

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

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

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

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

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

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

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

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

(A) an individual's employment or application for employment;

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

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

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

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

(10) any activity that involves collecting, maintaining, disclosing, selling, communicating, or using information for the purpose of evaluating a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living if done strictly in accordance with the

provisions of the Fair Credit Reporting Act, 15 U.S.C. § 1681–1681x, as may be amended, by:

(A) a consumer reporting agency;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(20) noncommercial activity of:

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

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

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

(D) an entity that provides an information service, including a press association or wire service; ~~or~~

~~(21) a public utility subject to the jurisdiction of the Public Utility Commission under 30 V.S.A. § 203, but only until July 1, 2026.~~

Sec. 12. EFFECTIVE DATES

(a) This section and Secs. 2 (public education and outreach), 3 (protection of personal information), 4 (data broker opt-out study), and 8 (study; Vermont Data Privacy Act) shall take effect on July 1, 2024.

(b) Secs. 1 (Vermont Data Privacy Act) and 7 (Age-Appropriate Design Code) shall take effect on July 1, 2025.

(c) Secs. 5 (Vermont Data Privacy Act middle applicability threshold) and 11 (utilities exemption repeal) shall take effect on July 1, 2026.

(d) Sec. 9 (private right of action) shall take effect on January 1, 2027.

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

(f) Sec. 10 (private right of action repeal) shall take effect on January 1, 2029.