Vermont’s Commitment to Privacy, Liberty & Innovation

Personal privacy, freedom, individual liberty, and equality are inalienable rights enshrined in our nation's founding Constitution. At the same time, we recognize that business innovation is critical to our economic growth and the prosperity of Vermont’s communities. Upholding these principles, the 2025 draft of Vermont’s Data Privacy & Online Surveillance Act reflects thousands of hours of stakeholder feedback. It centers on consumer protection while providing clear direction for businesses—ensuring they can not only comply with the law but also continue engaging with existing customers and attracting new ones.

This year’s draft remains grounded in the framework of Connecticut SB 6 (2022), as well subsequent amendments on consumer health and minor protections from Connecticut SB 3 (2023). Legislative Counsel and I have responded with a number of adjustments that address concerns from the business community while maintaining the core consumer protections expected by Vermonters.

We heard concerns that businesses worried that the bill restricted their ability to engage in direct marketing through various channels. Drawing on input from Vermont, other U.S. states, and the process surrounding the American Privacy Rights Act, we incorporated clearer distinctions between first- and third-party marketing, as well as between contextual and targeted advertising. We made clear that businesses can continue to use data they gather from their customers and website visitors to communicate and send ads.

We significantly revised the enforcement section. Now, consumers must first engage in intermediary steps with the Attorney General before pursuing a private right of action to address violations. Consumers cannot bring a private right of action against any company earning less than $25 million in annual revenue. Additionally, the private right of action continues to be both (1) limited in scope (anchored to violations of specific parts of the bill) and (2) limited in applicability - to data brokers (entities that sell personal data) as well as large data holders (businesses that collect the data of 100,000 Vermonters or more per year).

In keeping with evolving state privacy legislation, we adjusted several definitions, such as those for sensitive data and publicly available information.

Under the 2024 version, businesses that have already created a data protection assessment to comply with another state’s requirements would not need to craft a separate, Vermont-specific assessment. This interoperability provision now also extends to privacy policies.

We added exceptions allowing controllers and processors to use data for critical purposes, including conducting product recalls, performing research projects, carrying out necessary internal operations, and identifying and repairing technical errors.

In response to feedback that the bill was too lengthy, we reduced its length from 105 pages to 64. We also made slight structural adjustments to enhance overall readability.

We have maintained strong measures when it comes to consumers' most sensitive data, consumer health data, data of minors under 18, and situations that present heightened risks. These robust protections build upon the inalienable rights to personal privacy, freedom, individual liberty, and equality that are enshrined in our nation's founding Constitution.

Supporting Trustworthy & Resilient Businesses

At the same time, by streamlining requirements and fostering clear guidelines, we support business innovation and ensure that Vermont remains a competitive and attractive environment for enterprises to thrive. Privacy and data security are increasingly critical for consumer trust in business. This bill sets clear rules that enable Vermont businesses to gain that trust. Businesses that earn consumer trust gain a competitive advantage in the market and reduce their risks and costs by becoming more resilient and less likely to suffer from data breaches. This trust not only enhances their reputation but also contributes to lower vulnerability to security incidents, fostering a stronger and more secure economic landscape in Vermont.

Stay Informed & Engaged

Please note that the following policy language is a working draft and is not intended for public distribution. I invite and encourage stakeholders to schedule one-on-one discussions, submit redlines, and/or express a desire to testify once the legislative session begins.

Please complete this form if you would like to receive updates on the policies I am working on during the 2025-2026 session. Updates will include policy drafts, amendments, calls for feedback, responses to feedback, as well as other engagement opportunities. Expected 2025-2026 policy areas of focus include data privacy and surveillance, age-appropriate design code, algorithmic discrimination, artificial intelligence liability, and more. If you have any questions, please email me at mpriestley@leg.state.vt.us.

Vermont State Representative Monique Priestley mpriestley@leg.state.vt.us

Introduced by Representative Priestley of Bradford

Referred to Committee on

Date:

Subject: Commerce and trade; consumer protection; data privacy

Statement of purpose of bill as introduced: This bill proposes to provide data privacy protections to Vermonters.

An act relating to consumer data privacy and online surveillance

It is hereby enacted by the General Assembly of the State of Vermont:

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

CHAPTER 61A. VERMONT DATA PRIVACY AND ONLINE SURVEILLANCE ACT

§ 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) "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.

(3)(A) "Biometric data" means data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that allow or confirm the unique identification of the consumer, including:

(i) iris or retina scans;

(ii) fingerprints;

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

(iv) vein patterns;

(v) voice prints or vocal biomarkers; 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.

(4) "Broker-dealer" has the same meaning as in 9 V.S.A. § 5102.

(5) "Business associate" has the same meaning as in HIPAA.

(6) "Child" has the same meaning as in COPPA.

(7)(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 in response to a specific request, provided the request:

(i) is provided to the consumer in a clear and conspicuous disclosure;

(ii) includes a description of the processing purpose for which the consumer's consent is sought;

(iii) clearly distinguishes between an act or practice that is necessary to fulfill a request of the consumer and an act or practice that is for another purpose;

(iv) clearly states the specific categories of personal data that the controller intends to collect or process under each act or practice;

(v) clearly states the specific categories of personal data that the controller intends to collect or process under each act or practice; and

(vi) is accessible to a consumer with disabilities.

(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;

(iii) inaction of the consumer or the consumer's continued use of a service or product provided by the controller; or

(iv) an agreement obtained through the use of dark patterns.

(8)(A) "Consumer" means an individual who is a resident of the State.

(B) "Consumer" does not include an individual acting in a commercial or as an 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.

(9) "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.

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

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

(12) "Contextual advertising" or "contextual advertisement," as subject to provisions set forth in subsection 2418(g) of this chapter, means displaying or presenting an advertisement that does not vary based on the identity of the individual recipient and is based solely on:

(A) the immediate content of a webpage or online service within which the advertisement appears; or

(B) a specific request of the consumer for information or feedback.

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

(14) "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.

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

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

(17) "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."

(18) "Data broker" has the same meaning as in section 2430 of this title.

(19) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions that result in or materially affect access to, the provision or denial of, or the terms and conditions 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.

(20) "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) takes reasonable physical, technical, or administrative measures to ensure that the data cannot be used to reidentify 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, provided that such

reasonable measures for protected health information covered by HIPAA 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 reidentify 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 (20).

(21) "Financial institution" as used in subdivision 2417(a)(11) of this title, has the same meaning as in 15 U.S.C. § 6809;

(22) "First party" means a consumer-facing controller with which the consumer intends or expects to interact.

(23) "First-party advertising" means processing by a first party of its own first-party data for the purposes of advertising and marketing and is carried out:

(A) through direct communications with a consumer, such as direct mail, email, or text message communications;

(B) in a physical location operated by the first party; or

(C) through display or presentation of an advertisement on the first party's own website, application, or its other online content.

(24) "First-party data" means personal data collected directly from a consumer by a first party in compliance with this chapter, including based on a visit by the consumer to or use by the consumer of a website, a physical location, or an online service operated by the first party.

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

(26) "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.

(27) "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.

(28) "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.

(29) "Health care component" has the same meaning as in HIPAA.

(30) "Health care facility" has the same meaning as in 18 V.S.A. § 9432.

(31) "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, but excluding medical treatment recognized by nationally recognized medical associations, including the American Academy of Pediatrics and the American Medical Association;

(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.

(32) "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.

(33) "Hybrid entity" has the same meaning as in HIPAA.

(34) "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.

(35) "Independent trust company" has the same meaning as in 8 V.S.A. § 2401.

(36) "Investment adviser" has the same meaning as in 9 V.S.A. § 5102.

(37) "Large data holder" means a person who during the preceding calendar year processed the personal data of not fewer than 100,000 consumers.

(38) "Marketing measurement" means measuring and reporting on marketing performance or media performance by the controller, including processing personal data for measurement and reporting of frequency,

attribution, and performance, provided that such measurement data is not processed or transferred for any other purpose.

(39) "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.

(40) "Minor" means any consumer who is younger than 18 years of age.

(41) "Neural data" means information that is collected through biosensors and that could be processed to infer or predict mental states.

(42) "Nonpublic personal information" has the same meaning as in 15 U.S.C. § 6809.

(43)(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 (43).

(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, but not including the provision or use of an online service, product, or feature through use of an internet-connected physical product.

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

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

(46)(A) "Personal data" means any information, including derived data and unique identifiers, that is linked or reasonably linkable, alone or in combination with other information, 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.

(47)(A) "Precise geolocation data" means information derived from technology that reveals the past or present physical location of a consumer or device that identifies or is linked or reasonably linkable to one or more consumers with precision and accuracy 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;

(iii) a photograph, or metadata associated with a photograph or video, that cannot be linked to an individual; or

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

(48) "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.

(49) "Processor" means a person who processes personal data on behalf of:

(A) a controller;

(B) another processor; or

(C) a federal, state, tribal, or local government entity.

(50) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects, including an individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(51) "Protected health information" has the same meaning as in HIPAA.

(52)(A) "Publicly available information" means information that:

(i) is 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.

(B) "Publicly available information" does not include:

(i) biometric data collected by a business about a consumer without the consumer's knowledge;

(ii) information that is collated and combined to create a consumer profile that is made available to a user of a publicly available website either in exchange for payment or free of charge;

(iii) information that is made available for sale;

(iv) an inference that is generated from the information described in subdivision (ii) or (iii) of this subdivision (52)(B);

(v) any obscene visual depiction, as defined in 18 U.S.C. § 1460;

(vi) any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive data with respect to a consumer;

(vii) personal data that is created through the combination of personal data with publicly available information;

(viii) genetic data, unless otherwise made publicly available by the consumer to whom the information pertains;

(ix) information provided by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has maintained a reasonable expectation of privacy in the information, such as by restricting the information to a specific audience; or

(x) intimate images, authentic or computer-generated, known to be nonconsensual.

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

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

(55) "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.

(56) "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.

(57)(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.

(B) "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, with the consumer's consent, 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 publicly available information;

(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.

(58) "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, a mental or physical health condition, diagnosis, disability or treatment, status as pregnant, income level or indebtedness, 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 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 collected and analyzed concerning consumer health 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 used by the controller for a purpose other than to identify a specific consumer's physical or mental health condition or diagnosis;

(H) is biometric or genetic data;

(I) is collected from a known minor;

(J) is precise geolocation data;

(K) are keystrokes;

(L) is driving behavior; or

(M) is neural data.

(59)(A) "Targeted advertising" means displaying or presenting an online advertisement to a consumer or to a device identified by a unique persistent identifier, where the advertisement is selected based, in whole or in part, on known or predicted preferences, characteristics, behavior, or interests associated with the consumer or a device identified by a unique persistent

identifier. "Targeted advertising" includes displaying or presenting an online advertisement for a product or service based on the previous interaction of a consumer or a device identified by a unique persistent identifier with such product or service on a website or online service that does not share common branding with the website or online service displaying or presenting the advertisement, and marketing measurement related to such.

(B) "Targeted advertising" does not include:

(i) first-party advertising; or

(ii) contextual advertising.

(60) "Third party" means a person who collects personal data from another person who is not the consumer to whom the data pertains and is not a processor with respect to such data. "Third party" does not include a person who collects personal data from another entity if the entities are affiliates.

(61) "Trade secret" has the same meaning as in section 4601 of this title.

(62)(A) "Unique persistent identifier" means a technologically created identifier to the extent that such identifier is reasonably linkable to a consumer or a device that identifies or is linked or reasonably linkable to one or more consumers, including device identifiers, internet protocol addresses, cookies, beacons, pixel tags, mobile ad identifiers or similar technology customer numbers, unique pseudonyms, user aliases, telephone numbers, or other forms

of persistent or probabilistic identifiers that are linked or reasonably linkable to one or more consumers or devices.

(B) "Unique persistent identifier" does not include an identifier assigned by a controller for the sole purpose of giving effect to the exercise of affirmative consent or opt out by a consumer with respect to the collection or processing of personal data or otherwise limiting the collection or processing of personal data.

(63) "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.

§ 2416. APPLICABILITY

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

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

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

(b) Section 2425 of this chapter and the provisions of this chapter concerning consumer health data and consumer health data controllers apply to a person who conducts business in this State or a person who produces products or services that are targeted to residents of this State.

§ 2417. EXEMPTIONS

(a) This chapter does not apply to:

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

(2) protected health information under HIPAA;

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

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

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

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

(9) 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);

(10) 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);

(11) 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;

(12) a state or federally chartered bank or credit union, or an affiliate or subsidiary that is principally engaged in financial activities, as described in 18 U.S.C. § 1843(k);

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

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

(15) 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;

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

(17) 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) a press association or wire service.

(b) Controllers, processors, and consumer health data controllers that comply with the verifiable parental consent requirements of COPPA shall be

deemed compliant with any obligation to obtain parental consent pursuant to this chapter.

§ 2418. CONSUMER PERSONAL DATA RIGHTS

(a) A consumer shall have the right to:

(1) confirm whether a controller is processing the consumer's personal data and, if a controller is processing the consumer's personal data, access the personal data;

(2) obtain from a controller a list of third parties to which the controller has disclosed the consumer's personal data or, if the controller does not maintain this information in a format specific to the consumer, a list of third parties to which the controller has disclosed personal data;

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

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

(5) obtain a copy of the consumer's personal data processed by the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; and

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

(A) targeted advertising;

(B) the sale of personal data; or

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

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

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

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

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

(B) The consumer may designate an authorized agent by means of an internet link, browser setting, browser extension, global device setting, or other

technology that enables the consumer to exercise the consumer's rights under subdivision (a)(4) or (a)(6) of this section.

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

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

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

(C) If the consumer appointed an agent, the controller shall interact with the agent throughout the process and, with the exclusion of a data access request, not require the consumer to be involved in the fulfillment of the request.

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

(3)(A) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any 12-month period or after every time the controller make material changes to its personal data practices and policies.

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

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

(D) When a controller determines a consumer request is manifestly unfounded, excessive, or repetitive, the controller shall inform the consumer and share the controller's justification prior to disregarding the request or charging the consumer a processing fee. That notice shall include instructions for appealing the decision.

(4)(A) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (a)(1)–(5) of this section, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer or the consumer's agent that the controller is unable to authenticate the request to exercise the right or rights until the consumer provides additional information

reasonably necessary to authenticate the consumer and the consumer's request to exercise the right or rights.

(B) A controller shall not require authentication to exercise an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent.

(C) If a controller denies an opt-out request because the controller believes the request is fraudulent, the controller shall send a notice to the person who made the request disclosing that the controller believes the request is fraudulent, why the controller believes the request is fraudulent, and that the controller shall not comply with the request. If the request was placed through an agent, both the agent and the person who appointed the agent shall receive that notice.

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

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

(B) the employment of any dark pattern.

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

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

(2) Be conspicuously available to the consumer.

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

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

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

(f) In response to a consumer request under subdivision (a)(1) of this section, a controller shall not disclose the following information about a consumer, but shall instead inform the consumer with sufficient particularity that the controller has collected that type of information:

(1) Social Security number;

(2) driver's license number or other government-issued identification number;

(3) financial account number;

(4) health insurance account number or medical identification number;

(5) account password, security questions, or answers; or

(6) biometric data.

(g)(1) A controller may use the following types of information to display a contextual advertisement:

(A) technical specifications as are necessary for the ad to be delivered and displayed properly on a given device;

(B) a consumer's immediate presence in a geographic area with a radius not smaller than 10 miles, or an area reasonably estimated to include online activity from at least 5,000 users, but not including precise geolocation data; and

(C) the consumer's language preferences, as inferred from context, browser settings, or user settings.

(2) Notwithstanding subdivision (1) of this subsection, a controller shall not use personal data to make inferences about a consumer, profile a consumer, or for any other purpose, and the controller shall not prohibit a consumer from using technical means to obfuscate or change a consumer's physical location to specify a language preference.

§ 2419. DUTIES OF CONTROLLERS

(a) A controller shall:

(1) limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain:

(A) a specific product or service requested by the consumer to whom the data pertains; and

(B) a communication, that is not an advertisement, by the controller to the consumer reasonably anticipated within the context of the relationship between the controller and the consumer;

(2) establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue, including disposing of personal data in accordance with a retention schedule that requires the deletion of personal data when the data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected or processed; and

(3) provide an effective mechanism for a consumer to withdraw consent provided pursuant to this chapter that is at least as easy as the mechanism by which the consumer provided the consent.

(b)(1) A controller that offers any online service, product, or feature to a consumer whom the controller knows is a minor shall:

(A) use reasonable care to avoid any heightened risk of harm to minors caused by processing of personal data in the course of providing the online service, product, or feature;

(B) provide to the minor a conspicuous signal indicating that the controller is collecting the minor's precise geolocation data and make the signal available to the minor for the entire duration of the collection of the minor's precise geolocation data; and

(C) not process the personal data of a minor for the purposes of targeted advertising or sell the personal data of a minor.

(2) For purposes of this subsection (b), "knows" means a controller knows or should have known the consumer is a minor, including based upon:

(A) the self-identified age provided by the minor or the age provided by a third party; or

(B) any age or closely related proxy the business knows or has inferred, derived, attributed to, or associated with the consumer for any purpose, including marketing, advertising, or product development.

(3) Nothing in this chapter shall be construed to require:

(A) the affirmative collection of any personal data with respect to the age of users that a controller is not already collecting in the normal course of business; or

(B) a controller to implement an age gating or age verification functionality.

(c) A controller shall not:

(1) process sensitive data concerning a consumer except when the processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains;

(2) sell sensitive data;

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

(A) denying goods or services;

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

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

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

(5)(A) except as provided in subdivision (B) of this subdivision (5), process a consumer's personal data in a manner that discriminates against individuals or otherwise makes unavailable the equal enjoyment of goods or services on the basis of an individual's actual or perceived race, color, sex,

sexual orientation or gender identity, physical or mental disability, religion, ancestry, or national origin;

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

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

(ii) processing for the purpose of a controller's or processor's self-testing to prevent or mitigate unlawful discrimination or otherwise to ensure compliance with State or federal law; or

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

(d) Subsections (a)–(c) of this section shall not be construed to:

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

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

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

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

(ii) the third party uses the personal data only for purposes of facilitating a benefit to which the consumer is entitled and does not process or transfer the personal data for any other purpose.

(e) The sale of personal data shall not be considered functionally necessary to provide a financial incentive program. A controller shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

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

(A) lists the categories of personal data, including the categories of sensitive data, that the controller processes with a clear description of what data each category includes;

(B) describes the controller's purposes for processing each category of personal data the controller processes in a way that gives consumers a meaningful understanding of how each category of their personal data will be used;

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

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

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

(F) describes the length of time the controller intends to retain each category of personal data or, if it is not possible to identify the length of time, the criteria used to determine the length of time the controller intends to retain categories of personal data;

(G) specifies an email address or other online method by which a consumer can contact the controller that the controller actively monitors;

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

(I) provides a clear and conspicuous description of any processing of personal data in which the controller engages for the purposes of targeted advertising, sale of personal data to third parties, or profiling the consumer in

furtherance of decisions that produce legal or similarly significant effects concerning the consumer, and a procedure by which the consumer may opt out of this type of processing; and

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

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

(3) Whenever a controller makes a material change to the controller's privacy notice or practices, the controller must notify consumers affected by the material change with respect to any prospectively collected personal data and provide a reasonable opportunity for consumers to withdraw consent to any further materially different transfer of previously collected personal data under the changed policy. The controller shall take all reasonable electronic measures to provide notification regarding material changes to affected consumers, taking into account available technology and the nature of the relationship.

(4) A controller is not required to provide a separate Vermont-specific privacy notice or section of a privacy notice if the controller's general privacy notice contains all the information required by this subsection.

(5) The privacy notice must be posted online through a conspicuous hyperlink using the word "privacy" on the controller's website home page or on a mobile application's app store page or download page. A controller that maintains an application on a mobile or other device shall also include a hyperlink to the privacy notice in the application's settings menu or in a similarly conspicuous and accessible location. A controller that does not operate a website shall make the privacy notice conspicuously available to consumers through a medium regularly used by the controller to interact with consumers, including email.

(g) The method or methods under subdivision (f)(1)(J) of this section for submitting a consumer's request to a controller must:

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

(2) provide a clear and conspicuous link to a website where the consumer or an authorized agent may opt out from a controller's processing of the consumer's personal data pursuant to subdivision 2418(a)(6) of this title or,

solely if the controller does not have a capacity needed for linking to a webpage, provide another method the consumer can use to opt out, which may include an internet hyperlink clearly labeled "Your Opt-Out Rights" or "Your Privacy Rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request; and

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

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

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

(ii) for purposes of subdivision (i) of this subdivision (B), use of an internet protocol address to estimate the consumer's location may be considered sufficient to accurately determine residency.

(h) If a consumer or authorized agent uses a method under subdivision (f)(1)(J) of this section to opt out of a controller's processing of the consumer's personal data pursuant to subdivision 2418(a)(6) of this title and the decision conflicts with a consumer's existing controller-specific privacy setting or voluntary participation in a bona fide reward, club card, or loyalty program or

a program that provides premium features or discounts, the controller shall comply with the consumer's opt-out preference signal but may notify the consumer of the conflict and provide to the consumer the choice to confirm the controller-specific privacy setting or participation in the program.

§ 2420. DUTIES OF PROCESSORS

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

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

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

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

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

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

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

(1) be valid and binding on both parties;

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

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

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

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

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

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

(8)(A) allow the controller, the controller's designee, or a qualified and independent person the processor engages, in accordance with an appropriate

and accepted control standard, framework, or procedure, to assess the processor's policies and technical and organizational measures for complying with the processor's obligations under this chapter;

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

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

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

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

(B) collects directly from an individual.

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

(d)(1) For purposes of determining obligations under this chapter, a person is a controller with respect to processing a set of personal data and is subject to an action under section 2424 of this title to punish a violation of this chapter, if the person:

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

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

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

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

§ 2421. DATA PROTECTION ASSESSMENTS FOR PROCESSING ACTIVITIES THAT PRESENT A HEIGHTENED RISK OF HARM TO A CONSUMER

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

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

(2) the sale of personal data;

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

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

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

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

(D) other substantial injury to consumers; and

(4) the processing of sensitive data.

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

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

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

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

(c)(1) The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the

Attorney General pursuant to section 2424 of this title, and the controller shall make the data protection assessment available to the Attorney General.

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

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

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

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

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

(f) A controller shall update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of personal data

collected or processed and level of risk presented by the processing throughout the processing activity's lifecycle in order to:

(1) monitor for harm caused by the processing and adjust safeguards accordingly; and

(2) ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing.

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

§ 2422. DE-IDENTIFIED DATA

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

(1) take reasonable measures to ensure that the data cannot be used to reidentify 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;

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

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

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

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

(1) reidentify de-identified data; or

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

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

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

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

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

§ 2423. CONSTRUCTION OF DUTIES OF CONTROLLERS AND PROCESSORS

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

(1) comply with federal, state, or municipal laws, ordinances, or regulations, except as prohibited by 1 V.S.A. § 150;

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

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

(4) carry out obligations under a contract under subsection 2420(b) of this title for a federal or State agency or local unit of government;

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

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

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

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

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

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

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

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

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

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

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

(14) effectuate a product recall; or

(15) process personal data previously collected in accordance with this chapter such that the personal data becomes de-identified data, including to:

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

(B) identify and repair technical errors that impair existing or intended functionality;

(C) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party; or

(D) conduct a public or peer-reviewed scientific, historical, or statistical research project that is in the public interest and adheres to all relevant laws and regulations governing such research, including regulations for the protection of human subjects.

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

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

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

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

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

(d) This chapter shall not be construed to:

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

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

(B) under 12 V.S.A. § 1615;

(2) apply to any person's processing of personal data in the course of the person's solely personal or household activities;

(3) require an independent school as defined in 16 V.S.A. § 11(a)(8) or a private institution of higher education, as defined in 20 U.S.C. § 1001 et seq., to delete personal data or opt out of processing of personal data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution;

(4) require, for employee data, deletion of personal data that would unreasonably interfere with the ordinary business operations of the controller or unreasonably adversely affect the rights of another employee, including under this chapter or pursuant to the protections set forth in 21 V.S.A chapter 5; or

(5) require, for processors acting on the behalf of a federal, State, tribal, or local government entity, deletion of personal data or opt out of the

processing of personal data that would unreasonably interfere with the provision of government services by or the ordinary operation of a government entity.

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

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

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

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

(C) compliant with the antidiscrimination provisions set forth in subdivision 2419(c)(5) of this title.

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

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

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

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

(g) This chapter shall not be construed to require a controller, processor, or consumer health data controller to implement an age-verification or age-gating system or otherwise affirmatively collect the age of consumers.

§ 2424. 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, 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) Subject to the requirements of subdivisions (3) and (4) of this subsection (d), a consumer who is harmed by a data broker's or large data holder's violation of subsection 2419(c) of this title or section 2425 of this title may bring an action under subsection 2461(b) of this title in Superior Court for:

(i) the greater of $5,000.00 or actual damages;

(ii) injunctive relief;

(iii) punitive damages, in the case of an intentional violation;

(iv) reasonable costs and attorney's fees; and

(v) any other relief the court deems proper.

(B) No action may be taken under subsection 2461(b) of this title:

(i) for a violation of any provision of this chapter or rules adopted pursuant to this chapter other than what is specifically permitted in subdivision (A) of this subdivision (2); or

(ii) against a controller that is registered in the State and that earned less than $25 million in revenue in the previous calendar year.

(3) At least 65 days prior to the filing of any action pursuant to subdivision (2)(A) of this subsection, the consumer shall:

(A) notify the Attorney General of the alleged harm in a form and manner prescribed by the Attorney General, which, at minimum, shall require the name of the consumer and a reasonable description of the alleged violation and the harm suffered; and

(B) mail to the alleged violator a written demand letter that identifies the consumer and reasonably describes the alleged violation and the harm suffered, unless the alleged violator does not maintain a place of business in Vermont or does not keep assets in Vermont.

(4) Within 65 days after receiving the notice required by subdivision (3)(A) of this subsection, the Attorney General shall review the alleged harm to determine whether the claim is frivolous or nonfrivolous.

(A) If the Attorney General determines that the claim is frivolous, the Attorney General shall notify the consumer in writing, and the consumer is prohibited from proceeding with an action under subsection 2461(b) of this title for the alleged harm.

(B) If the Attorney General determines that the claim is nonfrivolous or does not issue a determination within 65 days after receiving notice, the consumer may proceed with an action pursuant to subdivision (2)(A) of this subsection (d).

(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;

(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.

§ 2425. CONFIDENTIALITY OF CONSUMER HEALTH DATA

Except as provided in subsections 2417(a) and (b) of this title and section 2423 of this title, no person shall:

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

(2) provide any processor with access to consumer health data unless the person and processor comply with section 2420 of this title; or

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

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

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

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

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

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

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

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

(5) methods for conducting data inventories; and

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

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

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

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

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

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

(2) the obligations controllers have to consumers;

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

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

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

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

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

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

(f) On or before December 15, 2027, the Attorney General shall assess the effectiveness of the implementation of the Act and submit a report to the House Committee on Commerce and Economic Development and the Senate Committee on Economic Development, Housing and General Affairs with its findings and recommendations, including any proposed draft legislation to address issues that have arisen since implementation.

Sec. 3. 9 V.S.A. § 2416(a) is amended to read:

(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 the preceding calendar year:

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

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

Sec. 4. 9 V.S.A. § 2416(a) is amended to read:

(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 the preceding calendar year:

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

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

Sec. 5. EFFECTIVE DATES

(a) This section and Sec. 2 (public education and outreach) shall take effect on July 1, 2025.

(b) Sec. 1 (Vermont Data Privacy Act) shall take effect on July 1, 2026.

(c) Sec. 3 (Vermont Data Privacy Act middle applicability threshold) shall take effect on July 1, 2027.

(d) Sec. 4 (Vermont Data Privacy Act low applicability threshold) shall take effect on July 1, 2028.