S.93

Introduced by Senators Chittenden, Beck, Cummings, Mattos and Ram Hinsdale

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

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 ACT

§ 2415. DEFINITIONS

As used in this chapter:

(1) "Abortion" means terminating a pregnancy for any purpose other than producing a live birth.

(2)(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 (2), "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.

(3) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under subdivisions 2418(a)(1)–(4) 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.

(4)(A) "Biometric data" means personal data generated by automatic measurements of an individual's unique biological patterns or characteristics that are used to identify a specific individual.

(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.

(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.

(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.

(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 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.

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

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

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

(14) "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."

(15) "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.

(16) "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 measures to ensure that the data cannot be associated with an individual;

(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 (16).

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

(18) "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.

(19) "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.

(20) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as may be amended.

(21) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

(22) "Institution of higher education" means any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

(23) "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.

(24) "Nonprofit organization" means any organization that is qualified for tax exempt status under I.R.C. § 501(c)(3), 501(c)(4), 501(c)(6), or 501(c)(12), or any corresponding internal revenue code of the United States, as may be amended,

(25) "Person" means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust, or other legal entity.

(26)(A) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual.

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

(27)(A) "Precise geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 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.

(28) "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.

(29) "Processor" means a person who processes personal data on behalf of a controller.

(30) "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.

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

(32) "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.

(33) "Publicly available information" means information that:

(A) is lawfully made available through federal, state, or local government records or widely distributed media; or

(B) a controller has a reasonable basis to believe that the consumer has lawfully made available to the general public.

(34) "Reproductive or sexual health care" means any health care-related services or products rendered or provided concerning a consumer's reproductive system or sexual well-being, including any such service or product rendered or provided concerning:

(A) an individual health condition, status, disease, diagnosis, diagnostic test or treatment;

(B) a social, psychological, behavioral, or medical intervention;

(C) a surgery or procedure, including an abortion;

(D) a use or purchase of a medication, including a medication used or purchased for the purposes of an abortion, a bodily function, vital sign, or symptom;

(E) a measurement of a bodily function, vital sign, or symptom; or

(F) an abortion, including medical or nonmedical services, products, diagnostics, counseling, or follow-up services for an abortion.

(35) "Reproductive or sexual health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

(36) "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.

(37)(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 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.

(38) "Sensitive data" means personal data that includes:

(A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status;

(B) consumer health data;

(C) the processing of genetic or biometric data for the purpose of uniquely identifying an individual;

(D) personal data collected from a known child;

(E) data concerning an individual's status as a victim of crime; and

(F) an individual's precise geolocation data.

(39)(A) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.

(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.

(40) "Third party" means a person, public authority, agency, or body, other than the consumer, controller, or processor or an affiliate of the processor or the controller.

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

§ 2416. APPLICABILITY

(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 100,000 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 25,000 consumers and derived more than 25 percent of the person's gross revenue from the sale of personal data.

(b) Section 2426 of this title and the provisions of this chapter concerning consumer health data and consumer health data controllers apply 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.

§ 2417. EXEMPTIONS

(a) Except as provided in subsection (c) of this section, this chapter shall not apply to any:

(1) body, authority, board, bureau, commission, district or agency of this State or of any political subdivision of this State;

(2) person who has entered into a contract with an entity described in subdivision (1) of this subsection to process consumer health data on behalf of the entity;

(3) nonprofit organization;

(4) institution of higher education;

(5) national securities association that is registered under 15 U.S.C. 78o-3 of the Securities Exchange Act of 1934, as may be amended;

(6) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and regulations adopted to implement that act;

(7) covered entity or business associate, as defined in 45 C.F.R. § 160.103;

(8) tribal nation government organization; or

(9) air carrier, as:

(A) defined in 49 U.S.C. § 40102, as may be amended; and

(B) regulated under the Federal Aviation Act of 1958, 49 U.S.C. § 40101 et seq. and the Airline Deregulation Act of 1978, 49 U.S.C. § 41713, as may be amended.

(b) The following information, data, and activities are exempt from this chapter:

(1) protected health information under HIPAA;

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

(3) identifiable private information:

(A) for purposes of 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; and

(B) that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(4) information that identifies a consumer in connection with the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research, as defined in 45 C.F.R. § 164.501, that is conducted in accordance with the standards set forth in this subdivision and in subdivision (3) of this subsection, or other research conducted in accordance with applicable law;

(5) 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;

(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 derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

(9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program, or qualified service organization, as specified in 42 U.S.C. § 290dd-2, as may be amended;

(10) information used for public health activities and purposes as authorized by HIPAA, community health activities, and population health activities;

(11) the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that

provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., as may be amended;

(12) personal data collected, processed, sold, or disclosed under and in compliance with:

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

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

(13) personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, as may be amended;

(14) data processed or maintained:

(A) in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, consumer health data controller, or third party, to the extent that the data is collected and used within the context of that role;

(B) as the emergency contact information of a consumer pursuant to this chapter, used for emergency contact purposes, or

(C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information

pursuant to subdivision (1) of this subsection (b) and used for the purposes of administering such benefits; and

(15) personal data collected, processed, sold, or disclosed in relation to price, route, or service, as such terms are used in the Federal Aviation Act of 1958, 49 U.S.C. § 40101 et seq., as may be amended, and the Airline Deregulation Act of 1978, 49 U.S.C.§ 41713, as may be amended.

(c) 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 RIGHTS; COMPLIANCE BY CONTROLLERS; APPEALS

(a) A consumer shall have the right to:

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

(2) 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;

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

(4) 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, where the processing is carried out by automated means, provided the controller shall not be required to reveal any trade secret; and

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

(A) targeted advertising;

(B) the sale of personal data, except as provided in subsection 2420(b) of this title; or

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

(b)(1) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice.

(2) A consumer may designate an authorized agent in accordance with section 2419 of this title to exercise the rights of the consumer to opt out of the processing of the consumer's personal data for purposes of subdivision (a)(5) of this section on behalf of the consumer.

(3) In the case of processing personal data of a known child, the parent or legal guardian may exercise the consumer rights on the child's behalf.

(4) In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship, or other protective arrangement, the guardian or the conservator of the consumer may exercise the rights on the consumer's behalf.

(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.

(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.

(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.

(4)(A) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (a)(1)–(4) of this section using commercially reasonable efforts, 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 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 be required to authenticate 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.

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

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

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

(d)(1) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision.

(2) The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section.

(3) Not later than 60 days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

(4) If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

§ 2419. AUTHORIZED AGENTS AND CONSUMER OPT-OUT

(a) A consumer may designate another person to serve as the consumer's authorized agent, and act on the consumer's behalf, to opt out of the processing of the consumer's personal data for one or more of the purposes specified in subdivision 2418(a)(5) of this title.

(b) The consumer may designate an authorized agent by way of, among other things, a technology, including an internet link or a browser setting, browser extension, or global device setting, indicating the consumer's intent to opt out of the processing.

(c) A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

§ 2420. CONTROLLERS' DUTIES; SALE OF PERSONAL DATA TO THIRD PARTIES; NOTICE AND DISCLOSURE TO CONSUMERS; CONSUMER OPT-OUT

(a) A controller:

(1) shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer;

(2) except as otherwise provided in this chapter, shall not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

(3) shall 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;

(4) shall not process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data concerning a known child, without processing the data in accordance with COPPA;

(5) shall not process personal data in violation of the laws of this State and federal laws that prohibit unlawful discrimination against consumers;

(6) shall provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation

of the consent, cease to process the data as soon as practicable, but not later than 15 days after the receipt of the request;

(7) shall not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge, and willfully disregards, that the consumer is at least 13 years of age but younger than 16 years of age; and

(8) shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

(b) Subsection (a) of this section shall not be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(c) A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(1) the categories of personal data processed by the controller;

(2) the purpose for processing personal data;

(3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) the categories of personal data that the controller shares with third parties, if any;

(5) the categories of third parties, if any, with which the controller shares personal data; and

(6) an active email address or other online mechanism that the consumer may use to contact the controller.

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the processing, as well as the manner in which a consumer may exercise the right to opt out of the processing.

(e)(1) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this chapter.

(2) The means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable

communication of the requests, and the ability of the controller to verify the identity of the consumer making the request.

(3) A controller shall not require a consumer to create a new account in order to exercise consumer rights but may require a consumer to use an existing account.

(4)(A) The means shall include:

(i) providing a clear and conspicuous link on the controller's website to an web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and

(ii) not later than January 1, 2026, allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the personal data, through an opt-out preference signal sent to the controller with the consumer's consent indicating the consumer's intent to opt out of any the processing or sale, by a platform, technology, or other mechanism that shall:

(I) not unfairly disadvantage another controller;

(II) not make use of a default setting, but rather require the consumer to make an affirmative, freely given, and unambiguous choice to opt out of any processing of the consumer's personal data pursuant to this chapter;

(III) be consumer-friendly and easy to use by the average consumer;

(IV) be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or State law or regulation; and

(V) enable the controller to accurately determine whether the consumer is a resident of this State and whether the consumer has made a legitimate request to opt out of any sale of the consumer's personal data or targeted advertising.

(B) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the personal data, through an opt-out preference signal sent in accordance with the provisions of subdivision (A) of this subdivision (e)(4) conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts, or club card program, 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.

(5) If a controller responds to consumer opt-out requests received pursuant to subdivision (4)(A) of this subsection by informing the consumer of

a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subsection (b) of this section for the retention, use, sale, or sharing of the consumer's personal data.

§ 2421. PROCESSORS' DUTIES; CONTRACTS BETWEEN CONTROLLERS AND PROCESSORS

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter, including:

(1) taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, to the extent reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests;

(2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a data broker security breach or security breach, as defined in section 2430 of this title, of the system of the processor, in order to meet the controller's obligations; and

(3) providing necessary information to enable the controller to conduct and document data protection assessments.

(b)(1) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller.

(2) The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties.

(3) The contract shall require that the processor:

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

(B) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(C) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

(D) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and

(E) make available to the controller upon the reasonable request of the controller, all information in the processor's possession necessary to demonstrate the processor's compliance with this chapter.

(4) A processor shall provide a report of an assessment to the controller upon request.

(c) This section shall not be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship, as described in this chapter.

(d)(1) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed.

(2) A person who is not limited in the person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to the instructions, is a controller and not a processor with respect to a specific processing of data.

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

(4) If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a

controller with respect to the processing and may be subject to an enforcement action under section 2425 of this title.

§ 2422. CONTROLLERS' DATA PROTECTION ASSESSMENTS; DISCLOSURE TO ATTORNEY GENERAL

(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 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 rights of 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, 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 include similar activities.

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

§ 2423. DE-IDENTIFIED AND PSEUDONYMOUS DATA; CONTROLLERS' DUTIES; EXCEPTIONS; APPLICABILITY OF CONSUMERS' RIGHTS; DISCLOSURE AND OVERSIGHT

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

(1) take reasonable measures to ensure that the data cannot be associated with an individual;

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

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

(b) This chapter shall not be construed to:

(1) require a controller or processor to re-identify de-identified data or pseudonymous data; or

(2) maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(c) This chapter shall not be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

(1) 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;

(2) 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; and

(3) does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(d) The rights afforded under subdivisions 2418(a)(1)–(4) of this title shall not apply to pseudonymous data in cases where the controller is able to

demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

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

§ 2424. CONSTRUCTION OF CONTROLLERS' AND PROCESSORS' DUTIES

(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;

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

(5) provide a product or service specifically requested by a consumer;

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

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

(8) 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;

(9) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious, or deceptive activities or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for the action;

(10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines, or similar independent oversight entities that determine:

(A) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(B) the expected benefits of the research outweigh the privacy risks; and

(C) whether the controller or consumer health data controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

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

(12) 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.

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

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

(2) effectuate a product recall;

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

(4) 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 consumer health data 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.

(c)(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.

(d)(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, 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.

(e) This chapter shall not be construed to:

(1) impose any obligation on a controller or processor 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 United States 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 purely personal or household activities; or

(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.

(f)(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) reasonably necessary and proportionate to the purposes listed in this section; and

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

(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) The data 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.

(g) 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 (f) of this section.

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

§ 2425. ENFORCEMENT BY ATTORNEY GENERAL; NOTICE OF VIOLATION; CURE PERIOD; REPORT; PENALTY

(a) The Attorney General shall have exclusive authority to enforce violations of this chapter.

(b)(1) During the period beginning on July 1, 2025 and ending on December 31, 2026, the Attorney General shall, prior to initiating any action for a violation of any provision of this chapter, issue a notice of violation to the controller or consumer health data controller if the Attorney General determines that a cure is possible.

(2) If the controller or consumer health data controller fails to cure the violation within 60 days after receipt of the notice of violation, the Attorney General may bring an action pursuant to this section.

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

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

(B) the nature of each violation;

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

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

(c) Beginning on January 1, 2027, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation described in subsection (b) of this section, consider:

(1) the number of violations;

(2) the size and complexity of the controller or processor;

(3) the nature and extent of the controller's or processor's processing activities;

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

(5) the safety of persons or property;

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

(7) the sensitivity of the data.

(d) This chapter shall not be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or any other law.

(e) Subjection to the exception in subsection (f) of this section, a violation of the requirements of this chapter shall constitute an unfair and deceptive act

in commerce in violation of section 2453 of this title and shall be enforced solely by the Attorney General, provided that a consumer private right of action under subsection 2461(b) of this title shall not apply to the violation.

(f) The Attorney General shall provide guidance to controllers and processors for compliance with the terms of the Vermont Data Privacy Act. Any processor or controller that, in the opinion of the Attorney General, materially complies with the guidance provided by the Attorney General shall not constitute an unfair and deceptive act in commerce.

§ 2426. CONSUMER HEALTH DATA PRIVACY

(a) Except as provided in subsections (b) and (c) of this section and subsections 2417(b) and (c) 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 2421 of this title;

(3) use a geofence to establish a virtual boundary that is within 1,750 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; or

(4) sell, or offer to sell, consumer health data without first obtaining the consumer's consent.

(b) Notwithstanding section 2416 of this title, subsection (a) of this section, and the provisions of sections 2415–2425 of this title, inclusive, concerning consumer health data and consumer health data controllers, apply to persons that conduct business in this state and persons that produce products or services that are targeted to residents of this state.

(c) Subsection (a) of this section shall not apply to any:

(1) body, authority, board, bureau, commission, district or agency of this State or of any political subdivision of this State;

(2) person who has entered into a contract with an entity described in subdivision (1) of this subsection to process consumer health data on behalf of the entity;

(3) institution of higher education;

(4) national securities association that is registered under 15 U.S.C. 78o-3 of the Securities Exchange Act of 1934, as may be amended;

(5) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and regulations adopted to implement that act;

(6) covered entity or business associate, as defined in 45 C.F.R. § 160.103;

(7) tribal nation government organization; or

(8) air carrier, as:

(A) defined in 49 U.S.C. § 40102, as may be amended; and

(B) regulated under the Federal Aviation Act of 1958, 49 U.S.C. § 40101 et seq. and the Airline Deregulation Act of 1978, 49 U.S.C. § 41713, as may be amended.

Sec. 2. EFFECTIVE DATE

This act shall take effect on July 1, 2026.