TO THE HONORABLE SENATE:

The Committee on Economic Development, Housing and General Affairs to which was referred House Bill No. 211 entitled "An act relating to data brokers and personal information" respectfully reports that it has considered the same and recommends that the Senate propose to the House that the bill be amended as follows:

First: In Sec. 1, 9 V.S.A. chapter 62, in subchapter 5, in section 2446, in subdivision (a)(4), by striking out subdivision (A) in its entirety and inserting in lieu thereof a new subdivision (A) to read as follows:

(A) the name and primary physical, ~~e-mail, and Internet addresses~~ email, and internet addresses and phone number of the data broker;

Second: In Sec. 1, 9 V.S.A. chapter 62, in subchapter 5, in section 2446, in subdivision (a)(4)(E), by striking out subdivision (ii) in its entirety and inserting in lieu thereof a new subdivision (ii) to read as follows:

(ii) in the past year, has shared consumers' data with or sold consumers' data to:

(I) a foreign actor;

(II) the federal government;

(III) other state or local governments;

(IV) law enforcement, unless the data was shared pursuant to a subpoena or other court order; or

(V) a developer of a GenAI system or model;

Third: In Sec. 1, 9 V.S.A. chapter 62, in subchapter 5, in section 2446, in subdivision (c)(3)(B), by striking out subdivision (i) in its entirety and inserting in lieu thereof a new subdivision (i) to read as follows:

(i) data subject to:

(I) Title V of the Gramm-Leach-Bliley Act, as amended, and regulations adopted to implement that act;

(II) the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., as may be amended; or

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

Fourth: In Sec. 1, 9 V.S.A. chapter 62, in subchapter 5, in section 2446, in subdivision (c)(3)(B), by striking out subdivision (vi) in its entirety and inserting in lieu thereof a new subdivision (vi) to read as follows:

(vi) processed solely in the data broker's capacity as a processor to:

(I) the State or a political subdivision of the State;

(II) a business with which the consumer has a direct relationship, as that term is defined in subdivision 2430(6)(B) of this chapter; or

(III) a governmental entity, or a business acting on behalf of either a governmental entity or another business, provided that the data broker is also a nonprofit organization established to provide enrollment data reporting services on behalf of postsecondary schools, as that term is defined in 16 V.S.A § 176(b); or

Fifth: By striking out Sec. 3, effective date, in its entirety and inserting in lieu thereof a new reader assistance heading and a new Sec. 3 to read as follows:

* * * Cybersecurity Advisory Council * * *

Sec. 3. 20 V.S.A. § 4662 is amended to read:

§ 4662. CYBERSECURITY ADVISORY COUNCIL

(a) Creation. There is created the Cybersecurity Advisory Council to advise on the State's cybersecurity infrastructure, best practices, communications protocols, standards, training, and safeguards.

(b) Membership. The Council shall be composed of the following members:

(1) the Chief Information Officer, who shall serve as the Chair or appoint a designee from the Council to serve as the Chair;

(2) the Chief Information Security Officer;

(3) a representative from a distribution or transmission utility, appointed by the Commissioner of Public Service;

(4) a representative from a State municipal water system, appointed by the Secretary of Natural Resources;

(5) a representative from a Vermont hospital, appointed by the President of the Vermont Association of Hospitals and Health Systems;

(6) a person representing a Vermont business related to an essential supply chain, appointed by the Chair of the Vermont Business Roundtable;

(7) the Director of Vermont Emergency Management or designee;

(8) the Governor's Homeland Security Advisor or designee;

(9) the Vermont Adjutant General or designee;

(10) the Attorney General or designee; ~~and~~

(11) the President of Vermont Information Technology Leaders or designee;

(12) the Chair of the House Committee on Energy and Digital Infrastructure;

(13) the Chair of the Senate Committee on Institutions; and

(14) a representative from the Judiciary, appointed by the Chief Justice of the Supreme Court.

* * *

Sixth: By adding a new section to be Sec. 3a to read as follows:

Sec. 3a. 2023 Acts and Resolves No. 71, Sec. 4 is amended to read:

Sec. 4. REPEAL

20 V.S.A. chapter 208 (cybersecurity) is repealed on June 30, ~~2028~~ 2033.

Seventh: By adding a new reader assistance heading and a new section to be Sec. 4 to read as follows:

* * * Data Privacy * * *

Sec. 4. 9 V.S.A. chapter 61A is added to read:

CHAPTER 61A. DATA PRIVACY

Subchapter 1. Vermont Data Privacy and Online Surveillance Act

§ 2415a. SHORT TITLE AND DEFINITIONS

(a) Short title. This subchapter shall be known and may be cited as the "Vermont Data Privacy and Online Surveillance Act."

(b) Definitions. As used in this subchapter:

(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 2415d(a)(1)–(4) of this subchapter 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 organization, 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 organization, 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) "Decision that produces any legal or similarly significant effect" means any decision made by the controller, or on behalf of the controller, that results in the provision or denial by the controller of any financial or lending

service, any housing, any insurance, any education enrollment or opportunity, any criminal justice, any employment opportunity, or any health care service.

(16) "Deidentified 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 deidentified 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 (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) "Neural data" means any information that is generated by measuring the activity of an individual's central nervous system.

(25) "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,

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

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

(B) "Personal data" does not include deidentified data or publicly available information.

(28)(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.

(29) "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.

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

(31) "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.

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

(33) "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 are not attributed to an identified or identifiable individual.

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

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

(ii) a controller has a reasonable basis to believe:

(I) a consumer has lawfully made available to the general public; or

(II) has been lawfully made available to the general public from widely distributed media.

(B) "Publicly available information" does not include any biometric data that can be associated with a specific consumer and were collected without the consumer's consent.

(35) "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.

(36) "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.

(37) "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.

(38)(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.

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

(A) data revealing:

(i) racial or ethnic origin, religious beliefs, sex life, sexual orientation, status as nonbinary or transgender, or citizenship or immigration status; or

(ii) a mental or physical health condition, diagnosis, disability, or treatment;

(B) consumer health data;

(C) genetic or biometric data or information derived therefrom;

(D) personal data collected from an individual the controller has actual knowledge, or willfully disregards, is a child;

(E) precise geolocation data;

(F) neural data;

(G) a consumer's financial account number, financial account log-in information, or credit card or debit card number that, in combination with any required access or security code, password, or credential, would allow access to a consumer's financial account; or

(H) government-issued identification number, including, but not limited to, Social Security number, passport number, State identification card number, or driver's license number, that applicable law does not require to be publicly displayed.

(40)(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.

(41) "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.

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

§ 2415b. APPLICABILITY

(a) Thresholds. Except as provided in subsection (b) of this section, this subchapter 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 controlled or processed the personal data of not fewer than 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction

(b) Health data applicability. Section 2415k of this subchapter and the provisions of this subchapter 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.

(c) Controlling law. In the event of a conflict between the provisions of this subchapter and any other law, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

§ 2415c. EXEMPTIONS

(a) Except as provided in subsection (c) of this section, this subchapter 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) candidate's committee or political committee, as those terms are defined in 17 V.S.A. § 2901;

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

(6) institution of higher education;

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

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

(9) tribal nation government organization;

(10) 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;

(11) 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; or

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

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

(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) personal data for purposes of 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 derived from any of the health care-related information listed in this subsection that is deidentified in accordance with the requirements for deidentification pursuant to HIPAA;

(8) 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;

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

(10) 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;

(11) 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;

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

(13) 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 subchapter, 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;

(14) 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;

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

(16) information included in a limited data set, as described in 45 C.F.R. § 164.514(e), as amended, to the extent such information is used, disclosed and maintained in the manner specified in 45 C.F.R.§ 164.514(e).

(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 subchapter.

§ 2415d. CONSUMER PERSONAL DATA RIGHTS

(a) Consumer rights. A consumer shall have the right to:

(1) confirm whether or not a controller is processing the consumer's personal data and access such personal data, including any inferences about the consumer derived from such personal data and whether a controller or processor is processing a consumer's personal data for the purposes of profiling to make a decision that produces any legal or similarly significant effect concerning a consumer, unless such confirmation or access would require the controller to reveal a trade secret or the controller is prohibited from disclosing such personal data under subsection (e) of this section;

(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;

(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 2415e(b) of this subchapter; or

(C) profiling in furtherance of any automated decision that produces any legal or similarly significant effect concerning the consumer;

(6) if the consumer's personal data were processed for the purposes of profiling in furtherance of any automated decision that produced any legal or similarly significant effect concerning the consumer, and if feasible:

(A) question the result of such profiling;

(B) be informed of the reason that such profiling resulted in such decision;

(C) review the consumer's personal data that were processed for the purposes of such profiling; and

(D) if the profiling decision concerned housing, taking into account the nature of the personal data and the purposes for which such personal data were processed, allow the consumer to correct any incorrect personal data that were processed for the purposes of such profiling and have the profiling decision reevaluated based on the corrected personal data; and

(7) obtain from the controller a list of the third parties to which such controller has sold the consumer's personal data or, if such controller does not maintain a list of the third parties to which such controller has sold the consumer's personal data, a list of all third parties to which such controller has

sold personal data, provided the controller shall not be required to reveal any trade secret.

(b) Exercising consumer rights.

(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) 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 the purposes specified in subdivision (a)(5) of this section.

(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.

(3) In the case of processing personal data:

(A) of a consumer who the controller has actual knowledge, or willfully disregards, is a child, the parent or legal guardian may exercise the consumer rights on the child's behalf; and

(B) 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) Controller compliance. Except as otherwise provided in this subchapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to this subchapter as follows:

(1) Timeline to respond. A controller:

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

(B) 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) Declining to take action. 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) Cost of information.

(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) Authentication of request.

(A) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (a)(1)–(4) or (6) 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) Third-party data. 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 subchapter; 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 subchapter.

(d) Appeals.

(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.

(e) Disclosure of certain information. A controller shall not disclose the following personal data in response to a request to exercise the consumer's rights pursuant to subdivision (a)(1) of this section and shall instead inform the consumer or the person exercising such right on behalf of the consumer, with sufficient particularity, that the controller has collected the consumer's:

(1) Social Security number;

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

(3) financial account number;

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

(5) account password;

(6) security question or answer thereto; or

(7) biometric data.

§ 2415e. DUTIES OF CONTROLLERS

(a) Data collection and processing. A controller shall:

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

(2) unless the controller obtains the consumer's consent, not process the consumer's personal data for any material new purpose that is neither reasonably necessary to, nor compatible with, the purposes that were disclosed to the consumer pursuant to subdivision (1) of this subsection, taking into account:

(A) the consumer's reasonable expectation regarding the personal data at the time the personal data were collected based on the purposes that were disclosed to the consumer pursuant to subdivision (1) of this subsection (a);

(B) the relationship that the new purpose bears to the purposes that were disclosed to the consumer pursuant to subdivision (1) of this subsection (a);

(C) the impact that processing the personal data for the new purpose might have on the consumer;

(D) the relationship between the consumer and the controller and the context in which the personal data were collected; and

(E) the existence of additional safeguards, including encryption or pseudonymization, in processing the personal data for the new purpose;

(3) 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) not process sensitive data concerning a consumer unless such processing is reasonably necessary in relation to the purposes for which such sensitive data are processed and without obtaining the consumer's consent or, in the case of the processing of sensitive data concerning a consumer who the controller has actual knowledge, or willfully disregards, is a child, without processing the data in accordance with COPPA;

(5) not process personal data in violation of any:

(A) law of this State that prohibits unlawful discrimination against consumers, and any evidence, or lack of evidence, concerning proactive antibias testing or any similar proactive effort to avoid processing data in violation of any such law, including any evidence or lack of evidence concerning the quality, efficacy, recency, and scope of any testing or effort, the results of which shall be relevant to any claim available for a violation of such law and any defense available thereto; or

(B) federal law that prohibits unlawful discrimination against consumers;

(6) 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) not sell the sensitive data of a consumer without the consumer's consent;

(8) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data, under circumstances where a controller has actual knowledge, and willfully disregards, that the consumer is at least 13 years of age but younger than 18 years of age; and

(9) not discriminate against a consumer for exercising any of the consumer rights contained in this subchapter, 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) Limitations. 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) Privacy notice.

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

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

(B) the purpose for processing personal data;

(C) a description of the means, established pursuant to subsection (e) of this section, for consumers to submit requests to exercise their consumer rights pursuant to this subchapter, including a description of how consumers may:

(i) exercise a consumer's rights under subsection 2415d(a) of this subchapter; and

(ii) appeal a controller's decisions with regard to requests to exercise such rights;

(D) the categories of personal data that the controller sells to third parties, if any;

(E) the categories of third parties, if any, to which the controller sells personal data;

(F) a clear and conspicuous disclosure of any:

(i) processing of personal data for purposes of targeted advertising; or

(ii) sale of personal data to a third party for purposes of targeted advertising;

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

(H) a statement disclosing whether the controller collects, uses, or sells personal data for the purpose of training large language models; and

(I) the most recent month and year during which the controller updated the privacy notice.

(2) A controller shall make the privacy notice required under subdivision (1) of this subsection publicly available:

(A) through a conspicuous hyperlink that includes the word "privacy":

(i) on the home page of the controller's internet web site, if the controller maintains an internet web site;

(ii) on the application store page or download page of a mobile device, if the controller maintains an application for use on a mobile device; and

(iii) on the application's settings menu or in a similarly conspicuous and accessible location, if the controller maintains an application for use on a mobile device or other device used to connect to the internet;

(B) through a medium in which the controller regularly interacts with consumers, including mail, if the controller does not maintain a web site;

(C) in each language in which the controller:

(i) provides any product or service that is subject to the privacy notice; or

(ii) carries out any activity that is related to any product or service described in subdivision (i) of this subdivision (C); and

(D) in a manner that is reasonably accessible to, and usable by, individuals with disabilities.

(3) Whenever a controller makes any retroactive material change to the controller's privacy notice or practices, the controller shall:

(A) notify the consumers affected by such material change with respect to any personal data to be collected after the effective date of such material change;

(B) provide a reasonable opportunity for the consumers described in subdivision (A) of this subdivision (3) to withdraw consent to any further and materially different collection, processing, or transfer of previously collected personal data following such material change; and

(C) take all reasonable electronic measures to provide the notice set forth in this subdivision (3) to the affected consumers, taking into account the technology available to the controller and the nature of the controller's relationship with such affected consumers.

(4) Nothing in this subsection shall be construed to require a controller to provide a privacy notice that is specific to this State if the controller provides a generally applicable privacy notice that satisfies the requirements established in this subsection.

(d) Providing consumers access to exercise rights.

(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 subchapter.

(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 a web page that enables a consumer, or an agent of the consumer, to opt out of the processing of the consumer's personal data for purposes of targeted advertising or any sale of the consumer's personal data; and

(ii) not later than January 1, 2027, 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 subchapter;

(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.

§ 2415f. PROCESSORS' DUTIES; CONTRACTS BETWEEN CONTROLLERS AND PROCESSORS

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

(1) taking into account the nature of processing and to the extent possible, to fulfill the controller's obligation to respond to consumer rights requests pursuant to subsection 2415d(a) of this subchapter;

(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 and impact assessments.

(b) Contractual terms.

(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 subchapter;

(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 subchapter.

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

(c) Liabilities. 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 subchapter.

(d) Processors performing as controllers.

(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 are 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 2415i of this subchapter.

§ 2415g. DATA PROTECTION AND IMPACT ASSESSMENTS; DISCLOSURE TO ATTORNEY GENERAL

(a) Generally. 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) Requirements.

(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 each data protection assessment the use of deidentified 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) Impact assessments for profiling. Each controller that engages in any profiling for the purposes of making a decision that produces any legal or similarly significant effect concerning a consumer shall conduct an impact assessment for the profiling. The impact assessment shall include, to the extent reasonably known by or available to the controller, as applicable:

(1) a statement by the controller disclosing the purpose, intended use cases, and deployment context of, and benefits afforded by, the profiling;

(2) an analysis of whether the profiling poses any known or reasonably foreseeable heightened risk of harm to a consumer, and, if so:

(A) the nature of such heightened risk of harm to a consumer; and

(B) the steps that have been taken to mitigate such heightened risk of harm to a consumer;

(3) a description of:

(A) the main categories of personal data processed as inputs for the purposes of such profiling; and

(B) the outputs such profiling produces;

(4) an overview of the main categories of personal data the controller used to customize the profiling, if the controller used data to customize the profiling;

(5) any metrics used to evaluate the performance and known limitations of the profiling;

(6) a description of any transparency measures taken concerning the profiling, including any measures taken to disclose to consumers that the controller is engaged in profiling while the controller is engaged in the profiling; and

(7) a description of the post deployment monitoring and user safeguards provided concerning such profiling, including, but not limited to, the oversight, use, and learning processes established by the controller to address issues arising from such profiling.

(d) Disclosure to Attorney General.

(1) The Attorney General may require that a controller disclose any data protection or impact assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data or impact assessment available to the Attorney General.

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

(3) Data protection and impact 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 or impact 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.

(e) Assessment efficiency and applicability.

(1) A single data protection or impact assessment may address a comparable set of processing operations that include similar activities.

(2) If a controller conducts a data protection or impact assessment for the purpose of complying with another applicable law or regulation, the data protection or impact assessment shall be deemed to satisfy the requirements established in this section if the data protection or impact assessment is

reasonably similar in scope and effect to the data protection or impact assessment that would otherwise be conducted pursuant to this section.

(3) Data protection and impact assessment requirements shall apply to processing activities created or generated after July 1, 2026, and are not retroactive.

§ 2415h. DEIDENTIFIED DATA

(a) Requirements. A controller in possession of deidentified data shall:

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

(2) publicly commit to maintaining and using deidentified data without attempting to reidentify the data; and

(3) contractually obligate any recipients of the deidentified data to comply with the provisions of this subchapter.

(b) Limitations. This subchapter shall not be construed to:

(1) require a controller or processor to reidentify deidentified data or pseudonymous data;

(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; or

(3) require a controller or processor to 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;

(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; and

(C) 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.

(c) Pseudonymous data. The rights afforded under subdivisions 2415d(a)(1)–(4) of this subchapter 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.

(d) Oversight when disclosing. A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

§ 2415i. CONSTRUCTION OF DUTIES

(a) Generally. This subchapter 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 reidentification;

(11) assist another controller, processor, consumer health data controller, or third party with any of the obligations under this subchapter; 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 are being processed; and

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

(b) Internal use of data. The obligations imposed on controllers, processors, or consumer health data controllers under this subchapter 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;

(4) process personal data for the purposes of profiling in furtherance of any automated decision that may produce any legal or similarly significant effect concerning a consumer, provided the personal data are:

(A) processed only to the extent necessary to detect or correct any bias that may result from processing the data for such purposes, the bias cannot effectively be detected or corrected without processing the data, and the data are deleted once the processing has been completed;

(B) processed subject to appropriate safeguards to protect the rights of consumers secured by the Constitution or laws of this State or of the United States;

(C) subject to technical restrictions concerning the reuse of the data and industry-standard security and privacy measures, including pseudonymization;

(D) subject to measures to ensure that the data are secure, protected, and subject to suitable safeguards, including strict controls concerning, and documentation of, access to the data, to avoid misuse and ensure that only authorized persons may access the data while preserving the confidentiality of the data; and

(E) not transmitted, transferred, or otherwise accessed by any third party;

(5) 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; or

(6) perform internal operations in accordance with the internal operations exception established in COPPA if the controller, processor, or

consumer health data controller is processing data in accordance with the exception.

(c) Evidentiary privilege.

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

(2) This subchapter 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) Third parties.

(1) A controller, processor, or consumer health data controller that discloses personal data to a processor or third-party controller pursuant to this subchapter shall not be deemed to have violated this subchapter if the processor or third-party controller that receives and processes the personal data violates this subchapter, 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 subchapter.

(2) A third-party controller or processor receiving personal data from a controller, processor, or consumer health data controller in compliance with this subchapter is not in violation of this subchapter 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) Clarifications. This subchapter 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) Personal data processing.

(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.

(3) 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 of this subsection.

(4) 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.

§ 2415j. ENFORCEMENT

(a) Generally.

(1) Subject to the exception in subsection (b) of this section, a violation of the requirements of this subchapter 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. This subchapter shall not be construed as providing the basis for, or be subject to, a private right of action for violations of this subchapter or any other law.

(2) 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.

(3) Beginning on January 1, 2028, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation of this subchapter, consider:

(A) the number of violations of the controller or processor;

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

(C) the nature and extent of the controller's or processor'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.

(b) Guidance. The Attorney General shall provide guidance to controllers and processors for compliance with the terms of the Vermont Data Privacy and Online Surveillance 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.

§ 2415k. CONSUMER HEALTH DATA PRIVACY

Except as provided in section 2415i of this subchapter and subsection 2415c(b) of this subchapter, 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 2415f of this subchapter;

(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; or

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

Eighth: By adding a new section to be Sec. 4a to read as follows:

Sec. 4a. DATA PRIVACY; ATTORNEY GENERAL; INITIAL CURE PERIOD

(a) During the period beginning on July 1, 2026, and ending on December 31, 2027, the Attorney General shall, prior to initiating any action for a violation of any provision of 9 V.S.A. chapter 61A, subchapter 1 (Data Privacy and Online Surveillance Act), issue a notice of violation to the controller or consumer health data controller if the Attorney General determines that a cure is possible.

(b) 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 9 V.S.A. chapter 61A, subchapter 1.

Ninth: By adding a new section to be Sec. 5 to read as follows:

Sec. 5. EFFECTIVE DATES

This act shall take effect on July 1, 2026, except that Sec. 1 (data breaches and data brokers) shall take effect on January 1, 2027.

(Committee vote: _____)

_____

Senator _____

FOR THE COMMITTEE