



**Substitute Senate Bill No. 4**

**Public Act No. 26-64**

***AN ACT CONCERNING CONSUMER PRIVACY AND PROTECTION.***

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective October 1, 2026*) As used in this section and sections 2 to 10, inclusive, of this act, unless the context otherwise requires:

(1) "Accessible deletion mechanism" means the mechanism established pursuant to subsection (a) of section 5 of this act;

(2) "Applicant" means any data broker that submits an application for an initial registration, or for a registration renewal, under subsection (b) of section 2 of this act;

(3) "Brokered personal data" means one or more of the following personal data elements concerning a consumer, if categorized or organized for sale or license to a third party: (A) Name; (B) address; (C) date of birth; (D) place of birth; (E) mother's maiden name; (F) unique biometric data (i) generated from measurement or technical analysis of a human body characteristic, including, but not limited to, a fingerprint, retina or iris image or other unique physical or digital representation of biometric data, and (ii) used by the owner or licensee of such unique biometric data to identify or authenticate the consumer; (G) name or

**Substitute Senate Bill No. 4**

address of a member of the consumer's immediate family or household; (H) Social Security number or other government-issued identification number; or (I) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty;

(4) "Business" (A) means (i) any person who regularly engages in commercial activities for the purpose of generating income, (ii) any bank, Connecticut credit union, federal credit union, out-of-state bank, out-of-state trust company or out-of-state credit union, as such terms are defined in section 36a-2 of the general statutes, and (iii) any other person who controls, is controlled by or is under common control with any person described in subparagraph (A)(i) or (A)(ii) of this subdivision, and (B) does not include any body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state;

(5) "Commissioner" means the Commissioner of Consumer Protection;

(6) "Consumer" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(7) "Data broker" means any business or, if such business is not an individual, any portion of such business that sells or licenses brokered personal data to another person;

(8) "Data service provider" means any person who maintains personal data on behalf of a registered data broker;

(9) "Deletion request" means any request submitted by a consumer under subparagraph (A)(i) of subdivision (1) of subsection (a) of section 5 of this act;

(10) "Department" means the Department of Consumer Protection;

**Substitute Senate Bill No. 4**

(11) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time;

(12) "License" (A) means to grant access to, or distribute, brokered personal data in exchange for consideration, and (B) does not include using any personal data for the sole benefit of the person who provided such personal data if such person maintains control over the use of such personal data;

(13) "Minor" means any consumer who is younger than eighteen years of age;

(14) "Participating consumer" means any consumer who submits a verified deletion request;

(15) "Person" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(16) "Personal data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(17) "Registered data broker" means any data broker that is actively registered as a data broker in accordance with the provisions of section 2 of this act; and

(18) "Unregistered data broker" means any data broker that is not actively registered as a data broker in accordance with the provisions of section 2 of this act.

Sec. 2. (NEW) (*Effective October 1, 2026*) (a) Except as provided in section 7 of this act, no data broker shall sell or license brokered personal data in this state on or after January 1, 2027, unless the data broker is actively registered with the Department of Consumer Protection in accordance with the provisions of this section.

***Substitute Senate Bill No. 4***

(b) Except as provided in subsection (d) of this section and section 7 of this act, a data broker that intends to sell or license brokered personal data in this state shall submit to the Department of Consumer Protection, in a form and manner prescribed by the Commissioner of Consumer Protection, an application for an initial registration as a data broker. Each application for an initial registration as a data broker shall be accompanied by an initial registration fee in the amount of two thousand five hundred dollars. Each initial registration issued pursuant to this subsection shall expire on December thirty-first of the year in which such initial registration was issued, and may be renewed for successive one-year terms upon submission of a registration renewal application made in the manner set forth in this subsection for an initial application and payment of a registration renewal fee in the amount of two thousand five hundred dollars. All fees collected under this subsection shall be deposited in the data broker registration account established in section 8 of this act.

(c) Except as provided in subsection (d) of this section, each application submitted to the Department of Consumer Protection under subsection (b) of this section shall disclose: (1) The applicant's name, mailing address and an actively monitored electronic mail address and telephone number; (2) the address of the applicant's primary Internet web site; (3) the address of a publicly accessible Internet web page on the applicant's primary Internet web site that (A) does not make use of any dark pattern, as defined in section 42-515 of the general statutes, as amended by this act, and (B) details how a consumer may exercise each of the rights afforded to the consumer under subsection (a) of section 42-518 of the general statutes, as amended by this act; (4) whether the applicant collects (A) minors' personal data, or (B) consumers' precise geolocation data or reproductive or sexual health data, as such terms are defined in section 42-515 of the general statutes, as amended by this act; (5) the measures the applicant will take to ensure that no personal data are sold or licensed in violation of the provisions of sections 1 to 10,

**Substitute Senate Bill No. 4**

inclusive, of this act or sections 42-515 to 42-526, inclusive, of the general statutes, as amended by this act; (6) whether, and to what extent, the applicant or any of its subsidiaries is regulated under (A) the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time, (B) Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., and the regulations adopted thereunder, as said act and such regulations may be amended from time to time, (C) section 38a-38 of the general statutes, or (D) the privacy, security and breach notification rules issued by the United States Department of Health and Human Services, 45 CFR Parts 160 and 164, as amended from time to time; (7) for a registration renewal application submitted on or after July 1, 2029, the statement the applicant most recently posted on a publicly accessible Internet web page on such applicant's primary Internet web site pursuant to section 6 of this act; (8) for a registration renewal application submitted on or after July 1, 2031, (A) whether the applicant has undergone an audit pursuant to subparagraph (A)(i) of subdivision (1) of subsection (d) of section 5 of this act, and (B) if the applicant has undergone an audit pursuant to subparagraph (A)(i) of subdivision (1) of subsection (d) of section 5 of this act, the most recent year for which the applicant submitted an audit report and the materials associated therewith to the department pursuant to subdivision (2) of subsection (d) of section 5 of this act; and (9) any other information the Commissioner of Consumer Protection requires for the purposes of this section.

(d) The Department of Consumer Protection may approve and renew an application for registration as a data broker in accordance with the terms of an agreement between the department and the Nationwide Multistate Licensing System.

Sec. 3. (NEW) (*Effective October 1, 2026*) No data broker shall sell or license any personal data in violation of the provisions of sections 1 to 10, inclusive, of this act or sections 42-515 to 42-526, inclusive, of the general statutes, as amended by this act. Each registered data broker

**Substitute Senate Bill No. 4**

shall establish a privacy policy which, at a minimum, shall include measures to ensure that such registered data broker does not sell or license any personal data in violation of the provisions of sections 1 to 10, inclusive, of this act or sections 42-515 to 42-526, inclusive, of the general statutes, as amended by this act.

Sec. 4. (NEW) (*Effective October 1, 2026*) The Commissioner of Consumer Protection shall establish, and periodically update, an Internet web page on the Department of Consumer Protection's Internet web site that: (1) Discloses, for each registered data broker, the information required under subsection (c) of section 2 of this act that was included in the application such registered data broker most recently submitted, and the department most recently approved for such registered data broker, under subsection (b) of section 2 of this act; and (2) provides access to the accessible deletion mechanism established by the commissioner pursuant to subsection (a) of section 5 of this act.

Sec. 5. (NEW) (*Effective October 1, 2026*) (a) (1) Not later than July 1, 2028, the Commissioner of Consumer Protection shall establish an accessible deletion mechanism program. As part of the accessible deletion mechanism program, the commissioner shall establish an accessible deletion mechanism that:

(A) Enables a consumer to (i) submit a deletion request, in a verifiable form and manner prescribed by the commissioner, without charge to the consumer and in any language spoken by a consumer for whom a registered data broker has collected personal data, that all registered data brokers and data service providers delete the consumer's personal data, and (ii) specifically exclude one or more registered data brokers, and all data service providers for such registered data broker or brokers, from the consumer's deletion request;

(B) Enables a consumer to (i) securely submit, in a form and manner prescribed by the commissioner, (I) the consumer's motor vehicle

***Substitute Senate Bill No. 4***

operator's license number, and (II) additional personal data to aid in processing the consumer's deletion request, (ii) determine the status of the consumer's deletion request, and (iii) not more frequently than once during any forty-five-day period, submit an update to the participating consumer's verified deletion request in a verifiable form and manner prescribed by the commissioner, without charge to such participating consumer and in any language spoken by a consumer for whom a registered data broker has collected personal data;

(C) Enables a registered data broker to determine whether a consumer has specifically excluded the registered data broker, and all data service providers for such registered data broker, from the consumer's deletion request or any update thereto;

(D) Does not enable a registered data broker that accesses the accessible deletion mechanism for the purposes set forth in subparagraph (C) of this subdivision to access any additional personal data by way of such accessible deletion mechanism;

(E) Is readily accessible and usable by consumers with disabilities;

(F) Incorporates reasonable security safeguards, including, but not limited to, administrative, physical and technical safeguards, to protect consumers' personal data from any unauthorized use, disclosure, access, destruction or modification by way of the accessible deletion mechanism; and

(G) Provides, in a manner that is readily understandable by consumers, (i) a description of what constitutes personal data and therefore may be subject to a deletion request, (ii) an explanation of the processes for a consumer to submit and update a deletion request, and (iii) a description of the actions required under subsections (b) and (c) of this section.

(2) (A) If a consumer submits the consumer's motor vehicle operator's

***Substitute Senate Bill No. 4***

license number to the commissioner for the purpose of verifying such consumer's deletion request or any update thereto, the commissioner shall use such consumer's motor vehicle operator's license number to verify such deletion request or update and for no other purpose. The commissioner shall not share, store or retain such consumer's motor vehicle operator's license number.

(B) Each deletion request and update thereto is confidential and shall not be deemed a public record for the purposes of the Freedom of Information Act, as defined in section 1-200 of the general statutes.

(b) On and after August 15, 2028, and except as provided in section 7 of this act, the Commissioner of Consumer Protection, or the commissioner's authorized agent, shall:

(1) Verify that the consumer who purportedly submitted a deletion request or update thereto actually submitted such deletion request or update by using such consumer's motor vehicle operator's license number and, following such verification, update the accessible deletion mechanism to inform each registered data broker that accesses the accessible deletion mechanism that such deletion request or update has been verified; and

(2) If the commissioner, or the commissioner's authorized agent, cannot verify that the consumer who purportedly submitted a deletion request or update thereto actually submitted such deletion request or update, specify that all registered data brokers, and all data service providers for such registered data brokers, that are not specifically excluded from such unverified deletion request or such unverified update (A) may retain any personal data such registered data brokers and data service providers maintain concerning such consumer, and (B) shall process such unverified deletion request or such unverified update as an exercise of such consumer's right under subparagraph (B) of subdivision (5) of subsection (a) of section 42-518 of the general statutes,

***Substitute Senate Bill No. 4***

as amended by this act.

(c) (1) On and after October 1, 2028, and except as provided in section 7 of this act, each registered data broker shall access the accessible deletion mechanism at least once every forty-five days to:

(A) Examine each deletion request or update thereto to determine whether such registered data broker, and all data service providers for such registered data broker, are specifically excluded from such deletion request or update; and

(B) (i) For each verified deletion request or verified update thereto that does not specifically exclude such registered data broker, and all data service providers for such registered data broker, and subject to the exceptions set forth in subdivision (5) of this subsection, delete any personal data such registered data broker maintains concerning the participating consumer and direct all data service providers that maintain any personal data concerning the participating consumer on behalf of such registered data broker to delete such personal data; or

(ii) For each unverified deletion request or unverified update thereto that does not specifically exclude such registered data broker, and all data service providers for such registered data broker, (I) retain any personal data such registered data broker maintains concerning the consumer, and (II) process such unverified deletion request or such unverified update, and direct all data service providers for such registered data broker to process such unverified deletion request or such unverified update, as an exercise of the consumer's right under subparagraph (B) of subdivision (5) of subsection (a) of section 42-518 of the general statutes, as amended by this act.

(2) At least once every forty-five days after a registered data broker first deletes a participating consumer's personal data pursuant to subparagraph (B)(i) of subdivision (1) of this subsection, repeat the

***Substitute Senate Bill No. 4***

actions required under subparagraph (B)(i) of subdivision (1) of this subsection unless:

(A) Such registered data broker verifies that the participating consumer has submitted a verified update to a verified deletion request such participating consumer previously submitted to the accessible deletion mechanism; and

(B) Such verified update specifically excludes such registered data broker and all data service providers for such registered data broker from the verified updated deletion request.

(3) The Commissioner of Consumer Protection may impose a fee on each registered data broker that accesses the accessible deletion mechanism for the purposes of performing such registered data broker's duties under subdivisions (1) and (2) of this subsection. Such fee shall be in an amount determined by the commissioner, but shall not exceed the cost of providing such access. All fees collected under this subdivision shall be deposited in the data broker registration account established in section 8 of this act.

(4) On and after October 1, 2028, and except as provided in subdivision (5) of this subsection, no registered data broker, and no data service provider for such registered data broker, that deletes a participating consumer's personal data pursuant to subparagraph (B)(i) of subdivision (1) of this subsection or subdivision (2) of this subsection shall maintain, use or disclose any personal data such registered data broker or data service provider subsequently acquires concerning the participating consumer.

(5) (A) No registered data broker who maintains a participating consumer's personal data, and no data service provider for such registered data broker, shall be required to delete the participating consumer's personal data, and may maintain, use or disclose such

***Substitute Senate Bill No. 4***

consumer's personal data, to the extent that maintaining, using or disclosing such participating consumer's personal data is reasonably necessary to (i) comply with any federal, state or municipal law, ordinance or regulation, (ii) comply with any civil, criminal or regulatory inquiry, investigation, subpoena or summons by any federal, state, municipal or other governmental authority, (iii) cooperate with any law enforcement agency concerning any conduct or activity that such registered data broker or data service provider reasonably and in good faith believes may violate any federal, state or municipal law, ordinance or regulation, (iv) investigate, establish, exercise, prepare for or defend any legal claim, (v) provide any product or service specifically requested by such participating consumer, (vi) perform pursuant to any contract to which such participating consumer is a party, including, but not limited to, by fulfilling the terms of a written warranty, (vii) take any step at the request of such participating consumer prior to entering into a contract, (viii) take any immediate step to protect any interest that is essential for the life or physical safety of such participating consumer or another individual, (ix) prevent, detect, protect against or respond to any security incident, identity theft, fraud, harassment, malicious or deceptive activity or any illegal activity, preserve the integrity or security of any system or investigate, report or prosecute those responsible for any such action, (x) engage in any 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, or a similar independent oversight entity, that determines that (I) maintaining such participating consumer's personal data is likely to provide substantial benefits that do not exclusively accrue to such registered data broker or data service provider, (II) the expected benefits of such research outweigh the privacy risks, and (III) such registered data broker or data service provider has implemented reasonable safeguards to mitigate any privacy risk associated with such research, (xi) assist any other person in performing any obligation imposed under sections 1 to 10,

**Substitute Senate Bill No. 4**

inclusive, of this act, (xii) conduct internal research to develop, improve or repair any product, service or technology, (xiii) effectuate a product recall, (xiv) identify and repair any technical error that impairs existing or intended functionality, or (xv) perform internal operations that are reasonably aligned with the expectations such participating consumer had, or reasonably anticipated, based on such participating consumer's existing relationship with such registered data broker.

(B) Except as provided in section 7 of this act, no registered data broker, or data service provider for such registered data broker, that maintains, uses or discloses a participating consumer's personal data for any purpose set forth in subparagraph (A) of this subdivision shall maintain, use or disclose the participating consumer's personal data for any other purpose.

(d) (1) Except as provided in section 7 of this act, not later than July 1, 2031, and triennially thereafter, each registered data broker shall, at the expense of such registered data broker, (A) retain an independent auditor to (i) audit the books of such registered data broker to determine whether such registered data broker is in compliance with the provisions of subsection (c) of this section, (ii) prepare an audit report disclosing the results of such audit, and (iii) submit such audit report, and any materials associated therewith, to such registered data broker, and (B) maintain each audit report, and any materials associated therewith, that are submitted to such registered data broker pursuant to subparagraph (A)(iii) of this subdivision for a period of at least six years beginning on the date on which such audit report and materials are submitted to such registered data broker.

(2) Except as provided in section 7 of this act, a registered data broker shall submit an audit report and the materials described in subparagraph (A)(iii) of subdivision (1) of this subsection to the Department of Consumer Protection, in a form and manner prescribed by the Commissioner of Consumer Protection, not later than five

**Substitute Senate Bill No. 4**

business days after the department sends notice to the registered data broker disclosing that the department requires such registered data broker to submit such audit report and materials to the department.

(e) The Commissioner of Consumer Protection may enter into a contract with one or more public or private entities (1) for any services necessary to implement the provisions of subsections (a) to (d), inclusive, of this section, (2) to administer the accessible deletion mechanism program established pursuant to subsection (a) of this section, or (3) to administer a multistate accessible deletion mechanism program.

Sec. 6. (NEW) (*Effective October 1, 2026*) Except as provided in section 7 of this act, not later than July 1, 2029, and annually thereafter, each business that was a registered data broker during the preceding calendar year shall post, in a form and manner prescribed by the Commissioner of Consumer Protection and on a publicly accessible Internet web page on such business's primary Internet web site, a statement disclosing the following information:

(1) The total number of deletion requests, inclusive of any updates thereto, that such business accessed during the preceding calendar year and that did not specifically exclude such business and all data service providers for such business;

(2) The total number of deletion requests described in subdivision (1) of this section to which such business responded by:

(A) Deleting personal data;

(B) Retaining personal data; or

(C) Deleting and retaining personal data; and

(3) If such business responded to one or more deletion requests

**Substitute Senate Bill No. 4**

described in subdivision (1) of this section by retaining personal data, the total number of such deletion requests for which such business retained personal data:

(A) On the basis of an exception set forth in subdivision (5) of subsection (c) of section 5 of this act; or

(B) On the basis of an exemption set forth in section 7 of this act.

Sec. 7. (NEW) (*Effective October 1, 2026*) (a) The provisions of sections 1 to 10, inclusive, of this act shall not apply to: (1) A consumer reporting agency, as defined in 15 USC 1681a(f), as amended from time to time, a person who furnishes information to a consumer reporting agency, as provided in 15 USC 1681s-2, as amended from time to time, or a user of a consumer report, as defined in 15 USC 1681a(d), as amended from time to time, to the extent that the consumer reporting agency, person or user engages in activities that are subject to regulation under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (2) a financial institution, an affiliate or a nonaffiliated third party, as such terms are defined in 15 USC 6809, as amended from time to time, to the extent that the financial institution, affiliate or nonaffiliated third party engages in activities that are subject to regulation under Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., and the regulations adopted thereunder, as said act and such regulations may be amended from time to time; (3) a business that collects information concerning a consumer if the consumer is or was (A) in a contractual relationship with the business, (B) an investor in the business, (C) a donor to the business, or (D) in any relationship with the business that is similar to the relationships described in subparagraphs (A) to (C), inclusive, of this subdivision; (4) a business that performs services for, or is acting as an agent or otherwise on behalf of, a business described in subdivision (3) of this subsection or a governmental entity; (5) a business collecting data used for purposes of the regulation of listed chemicals as set forth in 21 USC 830, as amended from time to time; (6) a candidate committee,

**Substitute Senate Bill No. 4**

national committee, party committee or political committee, as such terms are defined in section 9-601 of the general statutes; and (7) a covered entity or business associate, as defined in 45 CFR 160.103.

(b) No provision of sections 1 to 10, inclusive, of this act shall be construed to prohibit an unregistered data broker from engaging in any sale or licensing of brokered personal data if such sale or licensing exclusively involves: (1) Publicly available information that (A) concerns a consumer's business or profession, (B) is sold or licensed as part of a service that provides alerts for health or safety purposes, or (C) is lawfully available from any federal, state or local government record, unless such information is (i) collated and combined to create a consumer profile that is made available to a user of a publicly accessible Internet web site for compensation or free of charge, or (ii) used to generate inferences with respect to consumers; (2) providing digital access to any (A) journal, book, periodical, newspaper, magazine or news media, or (B) educational, academic or instructional work; (3) developing or maintaining an electronic commerce service or software; (4) providing directory assistance or directory information services as, or on behalf of, a telecommunications carrier; or (5) a one-time or occasional disposition of the assets of a business, or any portion of a business, as part of a transfer of control over the assets of the business that is not part of the ordinary conduct of such business or portion of such business.

Sec. 8. (NEW) (*Effective October 1, 2026*) There is established an account to be known as the "data broker registration account", which shall be a separate, nonlapsing account. The account shall contain any moneys required by law to be deposited in the account. Moneys in the account shall be expended by the Commissioner of Consumer Protection for the purposes of the accessible deletion mechanism program established pursuant to subsection (a) of section 5 of this act.

Sec. 9. (NEW) (*Effective October 1, 2026*) The Commissioner of  
**Public Act No. 26-64** **15 of 41**

**Substitute Senate Bill No. 4**

Consumer Protection may adopt regulations, in accordance with the provisions of chapter 54 of the general statutes, to implement the provisions of sections 2 to 8, inclusive, of this act.

Sec. 10. (NEW) (*Effective October 1, 2026*) The Commissioner of Consumer Protection, after providing notice and conducting a hearing in accordance with the provisions of chapter 54 of the general statutes, may impose a civil penalty of not more than two hundred dollars per day for each violation of any provision of sections 2 to 8, inclusive, of this act. Any civil penalties collected under this section shall be deposited in the data broker registration account established in section 8 of this act.

Sec. 11. (NEW) (*Effective October 1, 2026*) (a) As used in this section:

(1) "Consumer" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(2) "Consumer good" means any article that is purchased, leased, exchanged or received primarily for personal, family or household purposes;

(3) "Consumer service" means any service that is purchased, leased, exchanged or received primarily for personal, family or household purposes;

(4) "Discounted price" means any price for a consumer good or consumer service that is (A) established for, or offered to, a consumer or group of consumers, and (B) verifiably lower than the generally available, publicly disclosed and bona fide market price established for the consumer good or consumer service;

(5) "Person" means any individual, association, corporation, limited liability company, partnership, trust or other legal entity;

**Substitute Senate Bill No. 4**

(6) "Personal data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(7) "Price setting device" means any automated or programmed process that uses a consumer's personal data to establish a price for a consumer good or consumer service to be sold, leased, exchanged or provided to the consumer;

(8) "Retail seller" (A) means a retailer, as defined in section 12-407 of the general statutes, to the extent such retailer is engaged in making sales, at retail, of tangible personal property, and (B) includes, but is not limited to, a retail food establishment;

(9) "Surveillance pricing" means the practice of establishing a customized price for a consumer good or consumer service that is specific to a consumer based, in whole or in part, on the consumer's personal data collected (A) through any technology or technological method, system or tool, including, but not limited to, any biometric monitoring, camera, device tracking or sensor, that is capable of gathering personal data concerning a consumer's behavior, characteristics, location or other personal attributes in a physical or digital environment, and (B) by the person establishing the customized price either directly or indirectly by gathering, purchasing or otherwise acquiring such personal data from a third party; and

(10) "Third-party delivery service" means a company, organization or entity, outside of the operation of a retail food establishment's business, that facilitates delivery or online ordering services to customers of a retail food establishment.

(b) (1) Except as provided in subsection (d) of this section, any person doing business in the state who uses a price setting device for any reason other than to establish a discounted price for a consumer good or consumer service to be sold, leased, exchanged or provided as part of

***Substitute Senate Bill No. 4***

an online transaction, and who directly or indirectly advertises or promotes online a price established for a consumer good or consumer service by using a price setting device, labels a consumer good with such price online or publishes an online statement, display, image, offer or announcement disclosing such price, shall include in such online advertisement, promotion, label, statement, display, image, offer or announcement the following disclosure, or a substantially similar disclosure: "THIS PRICE WAS INCREASED BY A PRICE SETTING DEVICE USING YOUR PERSONAL DATA".

(2) The disclosure required under subdivision (1) of this subsection shall be readily visible to the average consumer.

(c) (1) Except as provided in subsection (d) of this section, no retail seller or third-party delivery service doing business in the state shall engage in surveillance pricing.

(2) Notwithstanding the provisions of subdivision (1) of this subsection, the following shall not be deemed to constitute surveillance pricing:

(A) Establishing for, or offering to, a consumer a discounted price for a consumer service for the purpose of retaining the consumer as a customer;

(B) Establishing for, or offering to, different consumers different prices for the same consumer good or consumer service due to (i) justifiable differences in the costs incurred in providing such consumer good or consumer service to such consumers, including, but not limited to, justifiable differences in consumer selections, delivery distances or delivery times, or (ii) justifiable temporal differences, including, but not limited to, justifiable temporal differences due to price fluctuations based on supply and demand; or

(C) Establishing for, or offering to, a consumer or group of consumers

***Substitute Senate Bill No. 4***

a discounted price for a consumer good or consumer service (i) based on publicly disclosed uniform terms and conditions that may be satisfied by any consumer, including, but not limited to, by signing up for a mailing list, disclosing personal data, registering for promotional communications or participating in a promotional event, (ii) that is available to all consumers who are members of a broadly defined group, including, but not limited to, veterans or members of the armed forces, senior citizens, students, teachers or residents of a specific area, or (iii) through a loyalty, membership or rewards program in which consumers must affirmatively enroll. The retail seller or third-party delivery service shall (I) prominently post the discounted price, and the uniform terms and conditions for such discounted price, on such retail seller's or third-party delivery service's Internet web site in language that is readily understandable by the average consumer, and (II) offer such discounted price to all consumers pursuant to the uniform terms and conditions posted on such retail seller's or third-party delivery service's Internet web site.

(d) The provisions of subsections (b) and (c) of this section shall not be construed to apply to:

(1) Any person licensed, authorized to operate or registered, or required to be licensed, authorized to operate or registered, pursuant to the insurance laws of this state;

(2) Any financial institution or affiliate thereof, as such terms are defined in 15 USC 6809, as amended from time to time, to the extent such financial institution or affiliate is subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., as amended from time to time; or

(3) Any bank, holding company or out-of-state bank, as such terms are defined in section 36a-2 of the general statutes, or out-of-state holding company, as defined in section 36a-410 of the general statutes, that directly or indirectly establishes an office in the state and is subject

**Substitute Senate Bill No. 4**

to the supervision of, or regulation by, the Banking Commissioner pursuant to title 36a of the general statutes.

(e) Any violation of the provisions of subsections (b) to (d), inclusive, of this section shall constitute an unfair or deceptive trade practice for the purposes of subsection (a) of section 42-110b of the general statutes and shall be enforced solely by the Attorney General. Nothing in this section shall be construed to create a private right of action or to provide grounds for an action under section 42-110g of the general statutes.

Sec. 12. Section 42-515 of the 2026 supplement to the general statutes, as amended by section 5 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

As used in this section and sections 42-516 to 42-526, inclusive, unless the context otherwise requires:

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

(2) "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. For the purposes of this subdivision, "control" and "controlled" mean (A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company, (B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or (C) 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 (1) to (4), inclusive, of subsection (a) of section 42-518, as amended by this act, is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

**Substitute Senate Bill No. 4**

(4) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data are generated to identify a specific individual.

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

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

(7) "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. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include (A) acceptance of general or broad terms of use or a similar document that contains descriptions of personal data processing along with other, unrelated information, (B) hovering over, muting, pausing or closing a given piece of content, or (C) agreement obtained through the use of dark patterns.

(8) "Consumer" means an individual who is a resident of this state. "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

***Substitute Senate Bill No. 4***

uses to identify a consumer's physical or mental health condition, diagnosis or status, and includes, but is not limited to, 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 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

(13) "Covered entity" has the same meaning as provided 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, but is not limited to, 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) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data (A) takes reasonable measures to

**Substitute Senate Bill No. 4**

ensure that such data cannot be associated with an individual, (B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

(17) "Facial recognition technology" means any technology that analyzes facial features in still images or video to uniquely and personally identify a specific individual.

[(17)] (18) "Gender-affirming health care services" has the same meaning as provided in section [52-571n] 52-571m.

[(18)] (19) "Gender-affirming health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services.

[(19)] (20) "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)] (21) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

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

[(22)] (23) "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.

**Substitute Senate Bill No. 4**

[(23)] (24) "Mental health facility" means any health care facility in which at least seventy per cent of the health care services provided in such facility are mental health services.

[(24)] (25) "Neural data" means any information that is generated by measuring the activity of an individual's central nervous system.

[(25)] (26) "Nonprofit organization" means any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time.

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

[(27)] (28) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

[(28)] (29) "Precise geolocation data" means information derived from technology, including, but not limited to, 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 one thousand seven hundred fifty feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

[(29)] (30) "Process" and "processing" mean 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.

**Substitute Senate Bill No. 4**

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

[(31)] (32) "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)] (33) "Protected health information" has the same meaning as provided in HIPAA.

[(33)] (34) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided such 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)] (35) "Publicly available information" (A) means information that (i) is [lawfully] made available [from] through federal, state or [municipal] local government records or to the general public from widely distributed media, or (ii) a controller or processor, or an affiliate of a controller or processor, has a reasonable basis to believe [(I) a] that the consumer has lawfully made available to the general public, [or (II) has been lawfully made available to the general public from widely distributed media,] and (B) does not include any (i) biometric data [that can be associated with a specific] about a consumer [and were] collected by a business without the consumer's [consent] knowledge, (ii) obscene visual depiction, as such term is used in 18 USC 1460, as amended from time to time, (iii) personal data that are created by combining any information described in subdivision (28) of this section with any information described in subparagraph (A) of this subdivision, (iv) genetic data, unless such genetic data are made publicly available by the

**Substitute Senate Bill No. 4**

consumer, (v) information provided by a consumer on a publicly accessible Internet web site or online service (I) which Internet web site or online service is made available to the general public for compensation or free of charge, and (II) where the consumer has maintained a reasonable expectation of privacy in such information, including, but not limited to, by restricting such information to a specific audience, (vi) intimate image, as such term is used in section 53a-189c, known to be nonconsensual, or (vii) intimate synthetically created image, as such term is used in section 53a-189d, known to be nonconsensual.

[(35)] (36) "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, but not limited to, 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, but not limited to, an abortion, (D) a use or purchase of a medication, including, but not limited to, a medication used or purchased for the purposes of an abortion, (E) a bodily function, vital sign or symptom, (F) a measurement of a bodily function, vital sign or symptom, or (G) an abortion, including, but not limited to, medical or nonmedical services, products, diagnostics, counseling or follow-up services for an abortion.

[(36)] (37) "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)] (38) "Reproductive or sexual health facility" means any health care facility in which at least seventy per cent of the health care-related services or products rendered or provided in such facility are reproductive or sexual health care.

**Substitute Senate Bill No. 4**

[(38)] (39) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include (A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller, (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer, (C) the disclosure or transfer of personal data to an affiliate of the controller, (D) 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, (E) 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 (F) 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)] (40) "Sensitive data" means personal data that includes (A) data revealing (i) racial or ethnic origin, (ii) religious beliefs, (iii) a mental or physical health condition, diagnosis, disability or treatment, (iv) sex life, sexual orientation or status as nonbinary or transgender, or (v) citizenship or immigration status, (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 wilfully disregards, is a child, (E) data concerning an individual's status as a victim of crime, as defined in section 1-1k, (F) precise geolocation data, (G) neural data, (H) 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 (I) government-issued identification number, including, but not limited to, Social Security number, passport number, state

**Substitute Senate Bill No. 4**

identification card number or driver's license number, that applicable law does not require to be publicly displayed.

[(40)] (41) "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 Internet web sites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include (A) advertisements based on activities within a controller's own Internet web sites or online applications, (B) advertisements based on the context of a consumer's current search query, visit to an Internet web site or online application, (C) advertisements directed to a consumer in response to the consumer's request for information or feedback, or (D) processing personal data solely to measure or report advertising frequency, performance or reach.

[(41)] (42) "Third party" means a person, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the processor or the controller.

[(42)] (43) "Trade secret" has the same meaning as provided in section 35-51.

Sec. 13. Subsection (a) of section 42-518 of the 2026 supplement to the general statutes, as amended by section 8 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) 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, but not limited to, 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

**Substitute Senate Bill No. 4**

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 (A) personal data provided by, or obtained about, the consumer, (B) publicly available information that is (i) collated and combined to create a consumer profile that is made available to a user of a publicly accessible Internet web site for compensation or free of charge, or (ii) made available for sale, or (C) any inference generated from the information described in subparagraph (B) of this subdivision; (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 such 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 subdivision (2) of subsection (a) of section 42-520, as amended by this act, 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

**Substitute Senate Bill No. 4**

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.

Sec. 14. Subsection (a) of section 42-520 of the 2026 supplement to the general statutes, as amended by section 9 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) (1) A controller shall: (A) 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; (B) 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 subparagraph (A) of this subdivision, taking into account (i) the consumer's reasonable expectation regarding such personal data at the time such personal data were collected based on the purposes that were disclosed to the consumer pursuant to subparagraph (A) of this subdivision, (ii) the relationship that such new purpose bears to the purposes that were disclosed to the consumer pursuant to subparagraph (A) of this subdivision, (iii) the impact that processing such personal data for such new purpose might have on the consumer, (iv) the relationship between the consumer and the controller and the context in which the personal data were collected, and (v) the existence of additional safeguards, including, but not limited to, encryption or pseudonymization, in processing such personal data for such new purpose; (C) establish, implement and maintain reasonable

***Substitute Senate Bill No. 4***

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; (D) 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 wilfully disregards, is a child, without processing such data in accordance with COPPA; (E) not process personal data in violation of any law of this state that prohibits unlawful discrimination against consumers, and any evidence, or lack of evidence, concerning proactive anti-bias testing or any similar proactive effort to avoid processing such data in violation of such law, including, but not limited to, any evidence or lack of evidence concerning the quality, efficacy, recency and scope of any such testing or effort, the results of such testing or effort and the response to the results of such testing or effort, shall be relevant to any claim available for a violation of such law and any defense available thereto; (F) not process personal data in violation of any federal law that prohibits unlawful discrimination against consumers; (G) 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 such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; (H) not sell the sensitive data of a consumer without the consumer's consent; and (I) 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, or wilfully disregards, that the consumer is at least thirteen years of age but younger than eighteen years of age. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 42-515 to 42-525, inclusive, as amended by this act, including denying goods or services, charging

**Substitute Senate Bill No. 4**

different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.

(2) Nothing in subdivision (1) of this subsection shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which 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.

(3) (A) No controller shall sell any consumer's precise geolocation data.

(B) The provisions of subparagraph (A) of this subdivision shall not be construed to apply to the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

Sec. 15. Subsection (a) of section 42-521 of the 2026 supplement to the general statutes, as amended by section 10 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) (1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under sections 42-515 to 42-525, inclusive, as amended by this act. Such assistance shall include: [(1)] (A) Taking into account the nature of processing and insofar as is possible, to fulfill the controller's obligation to respond to consumers' requests to exercise their rights under section 42-518, as amended by this act; [(2)] (B) 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

**Substitute Senate Bill No. 4**

to the security of processing the personal data and in relation to the notification of a breach of security, as defined in section 36a-701b, of the system of the processor, in order to meet the controller's obligations; and [(3)] (C) providing necessary information to enable the controller to conduct and document data protection assessments and impact assessments.

(2) (A) No third party shall sell any consumer's precise geolocation data.

(B) The provisions of subparagraph (A) of this subdivision shall not be construed to apply to the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

Sec. 16. Subsection (a) of section 42-524 of the 2026 supplement to the general statutes, as amended by section 12 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) (1) Nothing in sections 42-515 to 42-526, inclusive, as amended by this act, shall be construed to restrict a controller's, processor's or consumer health data controller's ability to: [(1)] (A) Comply with federal, state or municipal ordinances or regulations; [(2)] (B) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities; [(3)] (C) 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 ordinances or regulations; [(4)] (D) investigate, establish, exercise, prepare for or defend legal claims; [(5)] (E) provide a product or service specifically requested by a consumer; [(6)] (F) perform [under] pursuant to a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

**Substitute Senate Bill No. 4**

[(7)] (G) take steps at the request of a consumer prior to entering into a contract; [(8)] (H) 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)] (I) 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 any such action; [(10)] (J) 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)] (i) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller or consumer health data controller, [(B)] (ii) the expected benefits of the research outweigh the privacy risks, and [(C)] (iii) 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)] (K) assist another controller, processor, consumer health data controller or third party with any of the obligations under sections 42-515 to 42-526, inclusive, as amended by this act; or [(12)] (L) 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 such processing is [(A)] (i) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data are being processed, and [(B)] (ii) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(2) (A) A controller or consumer health data controller that uses any facial recognition technology on its premises to prevent, detect, protect against or respond to security incidents, identity theft, fraud,

**Substitute Senate Bill No. 4**

harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action shall: (i) Exclusively use such facial recognition technology to match still images or video to a database maintained exclusively by such controller or consumer health data controller; and (ii) post clearly legible signage at each entrance to the premises where the facial recognition technology described in subparagraph (A)(i) of this subdivision is in use, other than an entrance to an area where access is restricted to authorized employees, (I) alerting consumers entering such premises that facial recognition technology is in use at such premises, and (II) that includes a conspicuous hyperlink or quick response code that directs consumers to the facial recognition technology policy maintained by such controller or consumer health data controller.

(B) Each facial recognition technology policy maintained pursuant to subparagraph (A)(ii)(II) of this subdivision: (i) Shall include contact information for the office of the Attorney General; and (ii) may disclose the controller's or consumer health data controller's policies concerning interactions between such controller's or consumer health data controller's loss prevention officers and consumers.

Sec. 17. (NEW) (*Effective October 1, 2026*) As used in this section and sections 18 and 19 of this act:

(1) "Biological sample" (A) means any material that is derived from the human body and known to contain DNA, and (B) includes, but is not limited to, any human tissue, blood, urine or saliva;

(2) "Consumer" means any individual who is physically present in this state and a recipient, or a prospective recipient, of genetic testing;

(3) "De-identified data" means any data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified

***Substitute Senate Bill No. 4***

or identifiable individual if the direct-to-consumer genetic testing company that possesses such data (A) takes administrative and technical measures to ensure that such data cannot be associated with an individual, (B) publicly commits to possess and use such data exclusively in de-identified form and not to attempt to reidentify such data, and (C) contractually obligates any recipient of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision;

(4) "Direct-to-consumer genetic testing company" or "company" (A) means any person doing business in this state who, in the ordinary course of such business, (i) offers genetic testing directly to a consumer, or (ii) collects, uses or analyzes genetic data that a consumer has provided to such person, and (B) does not include any individual who (i) is licensed by this state to provide health care services, and (ii) while acting within the scope of such individual's practice, orders genetic testing for a medical purpose;

(5) "DNA" means deoxyribonucleic acid;

(6) "Express consent" means an affirmative response by a consumer to a clear, meaningful and prominent notice regarding the collection, use, retention or disclosure of the consumer's genetic data for a specific purpose;

(7) "Genetic data" (A) means any data, regardless of format, concerning an individual's genetic characteristics, (B) includes, but is not limited to, (i) any raw sequence data that result from sequencing all, or any portion of, an individual's DNA, (ii) any genotypic or phenotypic information that is obtained by analyzing an individual's raw sequence data, and (iii) any information that (I) concerns a condition affecting an individual's health, (II) the individual reports to a direct-to-consumer genetic testing company, and (III) the direct-to-consumer genetic testing company analyzes in connection with the individual's raw sequence data and uses for scientific research or product development, and (C)

**Substitute Senate Bill No. 4**

does not include de-identified data;

(8) "Genetic testing" means (A) any laboratory test performed on an individual's complete DNA sequence, or one or more of an individual's DNA regions, chromosomes, genes or gene products, for purposes of determining the presence or absence of any genetic characteristic, and (B) any interpretation of an individual's genetic data; and

(9) "Person" means any individual, association, corporation, limited liability company, partnership, trust or other legal entity.

Sec. 18. (NEW) (*Effective October 1, 2026*) A consumer shall have a property right in, and shall retain the right to exercise exclusive control over, any biological sample that is derived from the consumer's body and provided to, or used by, a direct-to-consumer genetic testing company, as well as the results of any genetic testing conducted on the consumer's DNA by a direct-to-consumer genetic testing company. Such right to exercise exclusive control includes, but is not limited to, the right to exercise exclusive control over the collection, use, retention, maintenance, disclosure or destruction of such biological sample and results.

Sec. 19. (NEW) (*Effective October 1, 2026*) (a) A direct-to-consumer genetic testing company shall:

(1) At all times transact its business and conduct its affairs in a manner that is consistent with a consumer's rights under section 18 of this act;

(2) Prior to accepting any biological sample, genetic data or payment from a consumer, disclose to the consumer the company's policies and procedures concerning the collection, use and disclosure of genetic data;

(3) Display, in a prominent and publicly accessible location on the company's Internet web site, a privacy notice disclosing such company's

***Substitute Senate Bill No. 4***

policies and procedures concerning the collection, use, access, disclosure, transfer, security, retention and deletion of a consumer's data and the consumer's consent thereto;

(4) Prior to collecting, using or disclosing a consumer's genetic data, obtain the consumer's express consent for such collection, use or disclosure after disclosing to such consumer (A) the company's policies and procedures concerning use of the genetic data such company collects from consumers, (B) the identity of each person who may access the results of genetic testing performed by the company, including, but not limited to, any vendor or service provider for such company who may access such results, and (C) the manner in which the company may disclose such consumer's genetic data;

(5) In addition to the express consent required under subdivision (4) of this subsection, separately obtain a consumer's express consent to (A) disclose or transfer the consumer's genetic data to any person other than a vendor or service provider for the company, prior to disclosing or transferring such genetic data to such person, (B) use the consumer's genetic data for any purpose other than the primary purpose for which the company offered genetic testing directly to such consumer, prior to using such genetic data for such other purpose, or (C) retain the consumer's biological sample for any period following completion of the genetic testing for which such consumer provided such biological sample, prior to retaining such biological sample for such period;

(6) Obtain informed consent from a consumer in accordance with the federal policy for the protection of human subjects under 45 CFR 46, as amended from time to time, for any disclosure or transfer of the consumer's genetic data to a third party for research purposes or research conducted under the control of the company for purposes of publication or generalizable knowledge;

(7) Not disclose the results of any genetic testing performed on a

***Substitute Senate Bill No. 4***

consumer's DNA to any person other than the consumer, unless (A) the company has obtained such consumer's express consent to such disclosure, or (B) such disclosure is made to a person acting pursuant to a court order, warrant or subpoena;

(8) Not disclose a consumer's genetic data to (A) the consumer's employer, (B) any person who, in the ordinary course of business, (i) offers health insurance, life insurance or long-term care insurance coverage in this state or any other state, or (ii) provides information or data to any insurer, as defined in section 38a-1 of the general statutes, health care center, as defined in section 38a-175 of the general statutes, or fraternal benefit society, as described in section 38a-595 of the general statutes, for purposes of underwriting or rating of risks, or (C) any third party which the company knows, or reasonably should know, intends to use such genetic data for purposes of marketing, including, but not limited to, targeted advertising;

(9) Implement reasonable security measures to protect a consumer's biological sample or genetic data from any unauthorized access, destruction, use, modification or disclosure; and

(10) Implement a process for a consumer to (A) access the consumer's genetic data from the company, (B) require the company to delete the consumer's genetic data, (C) require the company to destroy, and confirm that such company has destroyed, the consumer's biological sample, and (D) revoke the consumer's consent for (i) the company to use such consumer's genetic data for research purposes, or (ii) any third party to which the company has provided such consumer's genetic data to use such genetic data for research purposes.

(b) Any violation of subsection (a) of this section shall be deemed an unfair or deceptive trade practice under subsection (a) of section 42-110b of the general statutes and shall be enforced solely by the Attorney General. Nothing in this section shall be construed to create a private

**Substitute Senate Bill No. 4**

right of action or to provide grounds for an action under section 42-110g of the general statutes.

Sec. 20. (NEW) (*Effective October 1, 2026*) (a) As used in this section:

(1) "Cable operator" has the same meaning as provided in 47 USC 522, as amended from time to time;

(2) "Commercial advertisement" has the same meaning as such term is used in the Commercial Advertisement Loudness Mitigation Act, P.L. 111-311, as amended from time to time;

(3) "Consumer" means any person who is physically present in this state and is a recipient, or a prospective recipient, of a streaming video service;

(4) "Multichannel video programming distributor" has the same meaning as provided in 47 USC 522, as amended from time to time;

(5) "Person" means any individual, association, corporation, limited liability company, partnership, trust or other legal entity;

(6) "Streaming video service" means any service through which any video content, including, but not limited to, any video programming, is made available directly to consumers through a distribution method that uses the Internet protocol;

(7) "Television broadcast station" has the same meaning as provided in 47 USC 325, as amended from time to time; and

(8) "Video programming" has the same meaning as provided in 47 USC 613, as amended from time to time.

(b) On and after July 1, 2027, a streaming video service shall not transmit to a consumer the audio of a commercial advertisement at a volume that is louder than the volume of the video content that

***Substitute Senate Bill No. 4***

accompanies the commercial advertisement, consistent with the regulations adopted by the Federal Communications Commission pursuant to the Commercial Advertisement Loudness Mitigation Act, P.L. 111-311, for television broadcast stations, cable operators and other multichannel video programming distributors.

(c) Any violation of the provisions of subsection (b) of this section shall constitute an unfair trade practice for the purposes of subsection (a) of section 42-110b of the general statutes and shall be enforced solely by the Attorney General. The provisions of section 42-110g of the general statutes shall not apply to any such violation. Nothing in this section shall be construed as providing the basis for a private right of action for any violation of subsection (b) of this section.