General Assembly

February Session, 2022

Committee Bill No. 6

LCO No. **1770**

*01770SB00006GL *

Referred to Committee on GENERAL LAW

Introduced by:
(GL)

AN ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING.

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

Section 1. (NEW) (*Effective July 1, 2023*) As used in this section and sections 2 to 11, inclusive, of this act, unless the context otherwise requires:

(1) "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" or "controlled" means (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.

(2) "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 4 of this act is being made by

the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

(3) "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.

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

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

(6) "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 a general or broad terms of use or 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.

(7) "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 or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

(8) "Controller" means an individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data.

(9) "COPPA" means the Children's Online Privacy Protection Act of

1998, 15 USC 6501 et seq., as amended from time to time.

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

(11) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice.

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

(13) "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 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.

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

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

(16) "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.

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

(18) "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.

(19) "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.

(20) "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.

(21) "Processor" means an individual who, or legal entity that, processes personal data on behalf of a controller.

(22) "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.

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

(24) "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 is not attributed to an identified or identifiable individual.

(25) "Publicly available information" means information that is lawfully made available through federal, state or municipal government records or widely distributed media and information that a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

(26) "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.

(27) "Sensitive data" means personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (C) personal data

collected from a known child, or (D) precise geolocation data.

(28) "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.

(29) "Third party" means an individual or legal entity, such as a public authority, agency or body, other than the consumer, controller, processor or an affiliate of the processor or the controller.

Sec. 2. (NEW) (*Effective July 1, 2023*) The provisions of sections 1 to 11, inclusive, of this act apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year: (1) Controlled or processed the personal data of not less than sixty-five thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) controlled or processed the personal data of not less than twenty-five thousand consumers and derived more than twenty-five per cent of their gross revenue from the sale of personal data.

Sec. 3. (NEW) (*Effective July 1, 2023*) (a) The provisions of sections 1 to 11, inclusive, of this act do 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) nonprofit organization; (3) institution of higher education; (4) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; (5) nonpublic personal information collected, processed, sold or disclosed pursuant to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., and its implementing regulations, as both may be amended from time to time; (6) financial institution, as defined in 15 USC 6809(3)(A), as amended from time to time, to the extent such financial institution maintains personal information in the same manner as nonpublic personal information and as long as such financial institution does not use personal information for targeted advertising with third parties and does not share or sell personal information to a third party unless such sharing or sale is permitted under the provisions of sections 1 to 11, inclusive, of this act; or (7) hospital, as defined in section 38a-493 of the general statutes, whether nonprofit or for-profit.

(b) The following information and data is exempt from the provisions of sections 1 to 11, inclusive, of this act: (1) Protected health information under HIPAA; (2) patient-identifying information for purposes of 42 USC 290dd-2; (3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46; (4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law; (6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.; (7) patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time; (8) information derived from any of the health care related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; (9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time; (10) information used for public health activities and purposes as authorized by HIPAA; (11) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time; (13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time; (14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time; (15) 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 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 an individual under sections 1 to 11, inclusive, of this act 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 under subdivision (1) of this subsection and used for the purposes of administering such benefits; and (16) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Airline Deregulation Act, 49 USC 40101 et seq., as amended from time to time, by an air carrier subject to said act, to the extent sections 1 to 11, inclusive, of this act are preempted by Airline Deregulation Act, 49 USC 41713, as amended from time to time.

(c) Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to sections 1 to 11, inclusive, of this act.

Sec. 4. (NEW) (*Effective July 1, 2023*) (a) A consumer shall have the right to: (1) Confirm whether or not a controller is processing the consumer's personal data and to access such personal data; (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; and (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subsection (b) of section 6 of this act, or (C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(b) 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. A consumer may designate an authorized agent in accordance with section 5 of this act to exercise the rights of such consumer to opt out of the processing of such consumer's personal data for purposes of subdivision (5) of subsection (a) of this section on behalf of the consumer. In the case of processing personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

(c) Except as otherwise provided in sections 1 to 11, inclusive, of this act, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

(1) A controller shall respond to the consumer without undue delay, but not later than forty-five days after receipt of the request. The controller may extend the response period by forty-five additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial forty-five-day response period, together with the reason for the extension.

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

(3) Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. 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. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate the request 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 until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request.

(d) 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. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than sixty 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. 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.

Sec. 5. (NEW) (*Effective July 1, 2023*) A consumer may designate another person to serve as the consumer's authorized agent, and act on such consumer's behalf, to opt out of the processing of such consumer's personal data for one or more of the purposes specified in subdivision (5) of subsection (a) of section 4 of this act. The consumer may designate such authorized agent by way of, among other things, a technology, including, but not limited to, an Internet link or a browser setting, browser extension or global device setting, indicating such consumer's intent to opt out of such processing. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to authenticate, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf.

Sec. 6. (NEW) (*Effective July 1, 2023*) (a) A controller shall: (1) Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer; (2) except as otherwise provided in sections 1 to 11, inclusive, of this act, not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent; (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 without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA; (5) not process personal data in violation of the laws of this state and federal laws that prohibit 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 such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; and (7) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge of, 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 1 to 11, inclusive, of this act, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods and services to the consumer.

(b) Nothing in subsection (a) of this section 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. If a consumer exercises the consumer's right to opt out pursuant to subdivision (5) of subsection (a) of section 4 of this act, a controller may not sell the consumer's personal data to a third party as part of such program unless: (1) The sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled; (2) the sale of personal data to third parties is clearly disclosed in the terms of the program; and (3) the third party uses the personal data only for purposes of facilitating such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.

(c) A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes: (1) The categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (4) the categories of personal data that the controller shares with third parties, if any; (5) the categories of third parties, if any, with which the controller shares personal data; and (6) an active electronic mail address that the consumer may use to contact the controller.

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

(e) 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 sections 1 to 11, inclusive, of this act. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to authenticate the identity of the consumer making the request. 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. Any such means shall include:

(1) (A) Providing a clear and conspicuous link on the controller's

Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and

(B) During the period beginning July 1, 2023, and ending December 31, 2024, allowing a consumer to opt out of, and, beginning January 1, 2025, requiring a consumer to opt in or opt out of, the processing of personal data for the purposes of targeted advertising or the sale of personal data through an opt-in or opt-out preference, as applicable, signal sent with the consumer's consent by a platform, technology or mechanism to the controller indicating the consumer's intent to opt-in or opt-out, as applicable, of processing data for targeted advertising or the sale of the consumer's personal data. An opt-out preference signal mechanism provided pursuant to this subsection shall:

(i) Not permit the manufacturer of a platform, browser, device or any other product offering a universal opt-out mechanism to unfairly disadvantage another controller;

(ii) Require controllers to inform consumers about the opt-out choices available under sections 1 to 11, inclusive, of this act;

(iii) Not adapt a mechanism that is a default setting, but rather clearly represent the consumer's affirmative, freely given and unambiguous choice to opt out of the processing of personal data pursuant to sections 1 to 11, inclusive, of this act;

(iv) Be consumer-friendly, clearly described and easy to use by the average consumer;

(v) Be as consistent as possible with any other similar mechanism required by any federal or state law or regulation; and

(vi) Permit the controller to accurately authenticate the consumer as a resident of this state and determine that the mechanism represents a legitimate request to opt out of the sale of personal data.

(2) If a controller responds to consumer opt-out requests received pursuant to subdivision (1) 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.

Sec. 7. (NEW) (*Effective July 1, 2023*) (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under sections 1 to 11, inclusive, of this act. Such assistance shall include: (1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests; (2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as defined in section 36a-701b of the general statutes, of the system of the processor, in order to meet the controller's obligations; and (3) providing necessary information to enable the controller to conduct and document data protection assessments.

(b) 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. 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. The contract shall also require that the processor: (1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; (2) 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; (3)

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 sections 1 to 11, inclusive, of this act; (4) 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 (5) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 1 to 11, inclusive, of this act, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(c) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in sections 1 to 11, inclusive, of this act.

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processer with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. 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 such processing.

Sec. 8. (NEW) (*Effective July 1, 2023*) (a) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer 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 such 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 such intrusion would be offensive to a reasonable person, or (D) other substantial injury to consumers; and (4) the processing of sensitive data.

(b) 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 such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in sections 1 to 11, inclusive, of this act. Data protection assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200 of the general statutes. To the extent any information contained in a data protection assessment disclosed to the

Attorney General includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

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

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

(f) Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2023, and are not retroactive.

Sec. 9. (NEW) (*Effective July 1, 2023*) (a) Any controller in possession of de-identified data shall: (1) Take reasonable measures to ensure that the data cannot be associated with an individual; (2) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and (3) contractually obligate any recipients of the de-identified data to comply with all provisions of sections 1 to 11, inclusive, of this act.

(b) Nothing in sections 1 to 11, inclusive, of this act shall be construed to: (1) Require a controller or processor to re-identify de-identified data or pseudonymous data; or (2) maintain data in identifiable form, or collect, obtain, retain or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(c) Nothing in sections 1 to 11, inclusive, of this act shall be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller: (1) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data; (2) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and (3) does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(d) Consumer rights shall not apply to pseudonymous data in cases where the controller is able to demonstrate 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 such information.

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

Sec. 10. (NEW) (*Effective July 1, 2023*) (a) Nothing in sections 1 to 11, inclusive, of this act shall be construed to restrict a controller's or processor's ability to: (1) Comply with federal, state or municipal 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 or processor reasonably and in good faith believes may violate federal, state or municipal 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 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 any such 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, or similar independent oversight entities, that determines (A) if 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) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification; (11) assist another controller, processor or third party with any of the obligations under sections 1 to 11, inclusive, of this act; or (12) process personal data for reasons of public interest in the area of public health, but solely to the extent that such processing is (A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(b) The obligations imposed on controllers or processors under sections 1 to 11, inclusive, of this act shall not restrict a controller's or processor's ability to collect, use or retain data for internal use to: (1) Conduct internal research to develop, improve or repair products, services or technology; (2) effectuate a product recall; (3) identify and repair technical errors that impair existing or intended functionality; or (4) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers or processors under sections 1 to 11, inclusive, of this act shall not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this state. Nothing in sections 1 to 11, inclusive, of this act shall be construed to prevent a controller or processor 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) A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of sections 1 to 11, inclusive, of this act, is not in violation of said sections if the third-party controller or processor that receives and processes such personal data is in violation of said sections, provided, at the time of disclosing the personal data, the disclosing controller or processor did not have reason to believe that the recipient would violate said sections. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of sections 1 to 11, inclusive, of this act is likewise not in violation of said sections for the transgressions of the controller or processor from which such third-party controller or processor receives such personal data.

(e) Nothing in sections 1 to 11, inclusive, of this act shall be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right to freedom of speech under the First Amendment to the United States Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

(f) Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is: (1) Reasonably necessary and proportionate to the purposes listed in this section; and (2) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section. 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 such collection, use or retention. Such 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 such collection, use or retention of personal data.

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

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

Sec. 11. (NEW) (*Effective July 1, 2023*) (a) The Attorney General shall have exclusive authority to enforce violations of sections 1 to 10, inclusive, of this act.

(b) During the period beginning on July 1, 2023, and ending on December 31, 2024, the Attorney General shall, prior to initiating any action for a violation of any provision of sections 1 to 10, inclusive, of this act, issue a notice of violation to the controller if the Attorney General determines that a cure is possible. If the controller fails to cure such violation within sixty days of receipt of the notice of violation, the Attorney General may bring an action pursuant to this section.

(c) Nothing in sections 1 to 10, inclusive, of this act shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or any other law.

(d) A violation of the requirements of sections 1 to 10, inclusive, of this act shall constitute an unfair trade practice for purposes of section 42-110b of the general statutes and shall be enforced solely by the

Attorney General, provided the provisions of section 42-110g of the general statutes shall not apply to such violation.

This act shall take effect as follows and shall amend the following sections:

Section 1	*July 1, 2023*	New section
Sec. 2	*July 1, 2023*	New section
Sec. 3	*July 1, 2023*	New section
Sec. 4	*July 1, 2023*	New section
Sec. 5	*July 1, 2023*	New section
Sec. 6	*July 1, 2023*	New section
Sec. 7	*July 1, 2023*	New section
Sec. 8	*July 1, 2023*	New section
Sec. 9	*July 1, 2023*	New section
Sec. 10	*July 1, 2023*	New section
Sec. 11	*July 1, 2023*	New section

Statement of Purpose:

To: (1) Establish (A) a framework for controlling and processing personal data, and (B) responsibilities and privacy protection standards for data controllers and processors; and (2) grant consumers the right to (A) access, correct, delete and obtain a copy of personal data, and (B) opt out of the processing of personal data for the purposes of (i) targeted advertising, (ii) certain sales of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning consumers.

[Proposed deletions are enclosed in brackets. Proposed additions are indicated by underline, except that when the entire text of a bill or resolution or a section of a bill or resolution is new, it is not underlined.]

Co-Sponsors: SEN. LOONEY, 11th Dist.; SEN. DUFF, 25th Dist.
SEN. ANWAR, 3rd Dist.; SEN. CABRERA, 17th Dist.
SEN. CASSANO, 4th Dist.; SEN. COHEN, 12th Dist.
SEN. DAUGHERTY ABRAMS, 13th Dist.; SEN. FLEXER, 29th Dist.
SEN. FONFARA, 1st Dist.; SEN. HASKELL, 26th Dist.
SEN. KUSHNER, 24th Dist.; SEN. LESSER, 9th Dist.
SEN. LOPES, 6th Dist.; SEN. MARONEY, 14th Dist.
SEN. MCCRORY, 2nd Dist.; SEN. MILLER P., 27th Dist.
SEN. MOORE, 22nd Dist.; SEN. SLAP, 5th Dist.

SEN. WINFIELD, 10th Dist.; REP. DATHAN, 142nd Dist.

S.B. 6