Senate

General Assembly

File No. 238

February Session, 2022

Substitute Senate Bill No. 6

Senate, March 31, 2022

The Committee on General Law reported through SEN. MARONEY of the 14th Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

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., 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.

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

(11) "Dark pattern" (A) means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and (B) includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

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

(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), 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.

(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 (A) is lawfully made available through federal, state or municipal government records or widely distributed media, and (B) 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 or 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 seventy-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) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; or (6) 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 section 19a-127o of the general statutes and 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, community health activities and population

health activities; (11) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 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 the 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 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, provided such controller shall not be required to reveal any trade secret; and (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subsection (b) of section 6 of this act, or (C) profiling in furtherance of solely automated 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 and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 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, once per consumer during any twelve-month period. 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.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision (3) of subsection (a) of this section by (A) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the

business's records and not using such retained data for any other purpose pursuant to the provisions of sections 1 to 11, inclusive, of this act, or (B) opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of sections 1 to 11, inclusive, of this act.

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

(A) (i) 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

(ii) Not later than January 1, 2025, allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall:

(I) Not unfairly disadvantage another controller;

(II) Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of such consumer's personal data pursuant to sections 1 to 11, inclusive, of this act;

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

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

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

(B) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent in accordance with the provisions of subparagraph (A) of this

subdivision conflicts with the consumer's existing business-specific privacy setting or participation in a business's financial incentive program, the business shall comply with such consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such business-specific privacy setting or participation in such business's financial incentive program.

(2) If a controller responds to consumer opt-out requests received pursuant to subparagraph (A) of 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 processor 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) The rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 4 of this act shall not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing 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 under a contract to which a consumer is a party, including fulfilling the terms of a written warranty; (7) take steps at the request of a consumer prior to entering into a contract; (8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis; (9) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for 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 that determines, or similar independent oversight entities that determine, (A) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller, (B) the expected benefits of the research outweigh the privacy risks, and (C) whether the controller 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, community health or population 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. Not later than February 1, 2024, the Attorney General shall submit a report, in accordance with section 11-4a of the general statutes, to the joint standing committee of the General Assembly having cognizance of matters relating to general law disclosing: (1) The number of notices of violation the Attorney General has issued; (2) the nature of each violation; (3) the number of violations that were cured during the sixty-

day cure period; and (4) any other matter the Attorney General deems relevant for the purposes of such report.

(c) Beginning on January 1, 2025, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation described in subsection (b) of this section, consider: (1) The number of violations; (2) the size and complexity of the controller or processor; (3) the nature and extent of the controller's or processor's processing activities; (4) the substantial likelihood of injury to the public; and (5) the safety of persons or property.

(d) 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.

(e) 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.

Sec. 12. (*Effective from passage*) (a) Not later than September 1, 2022, the chairpersons of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall convene a working group to:

(1) Study how HIPAA-adjacent data is handled and recommend legislation, if any, that is necessary to ensure the protection of HIPAA-adjacent data;

(2) Study algorithmic decision-making and make recommendations concerning the proper use of data to reduce bias in such decision-making; and

(3) Study other topics concerning data privacy.

(b) The chairpersons of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall

serve as the chairpersons of the working group, and shall jointly appoint the members of the working group. Such members shall include, but need not be limited to:

(1) Representatives from industry, academia, consumer advocacy groups, small and large companies and the office of the Attorney General; and

(2) Attorneys with experience in privacy law.

(c) The administrative staff of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall serve as administrative staff of the working group.

(d) Not later than January 1, 2023, the working group shall submit a report on its findings and recommendations to the joint standing committee of the General Assembly having cognizance of matters relating to general law, in accordance with the provisions of section 11-4a of the general statutes. The working group shall terminate on the date that it submits such report or January 1, 2023, whichever is later.

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
Sec. 12	*from passage*	New section

Statement of Legislative Commissioners:

In Section 1(12), "a consumer" was changed to "the consumer" for consistency; in Section 1(25), Subpara. designators were inserted, and

"information that" was deleted, for clarity; in Section 1(29), "controller," was changed to "controller or", for clarity; in Section 4(a)(1), "data and to" was changed to "data and", for clarity; in Section 4(c)(1), "period, together with" was changed to "period and of", for clarity; in Section 6(a)(7), "of" was deleted, for clarity, and "and" was changed to "or", for consistency; in Section 9(d), "that" was inserted, for clarity; in Section 10(a)(6), "under" was inserted, for clarity; and in Sections 10(a)(10)(A) and 10(a)(10)(C), "if" was changed to "whether", for clarity.

GL *Joint Favorable Subst.*

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact:

Agency Affected	Fund-Effect	FY 23 $	FY 24 $
Attorney General	GF - Cost	397,011	397,011
State Comptroller - Fringe Benefits[1]	GF - Cost	59,584	59,584

Note: GF=General Fund

Municipal Impact: None

Explanation

The bill establishes a mechanism for managing consumer data privacy requirements for private individuals. It authorizes the attorney general to bring an action to enforce the bill's requirements, under the Connecticut Unfair Trade Practices Act (CUTPA), to be enforced solely by the Office of the Attorney General (OAG).

Implementation of this new data management program would result in total annualized state costs of $456,595, including fringe benefits, for OAG to enforce based on the number of new actions anticipated under the bill. These costs are associated with one new legal investigator (with an annual salary of $89,234), an administrative assistant (with a salary of $57,777), and costs of $250,000 to contract with outside privacy experts.

The bill makes other changes that have no fiscal impact.

[1]The fringe benefit costs for most state employees are budgeted centrally in accounts administered by the Comptroller. The estimated active employee fringe benefit cost associated with most personnel changes is 40.53% of payroll in FY 23.

The Out Years

The annualized ongoing fiscal impact identified above would continue into the future subject to inflation.

OLR Bill Analysis

sSB 6

AN ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING.

SUMMARY

This bill establishes a framework for controlling and processing personal data. Among other things, it:

1. sets responsibilities and privacy protection standards for data controllers (those that determine the purpose and means of processing personal data) and processors (those that process data for a controller);

2. gives consumers the right to access, correct, delete, and get a copy of personal data and to opt out of the processing of personal data for certain purposes (e.g., targeted advertising);

3. requires controllers to conduct data protection assessments;

4. authorizes the attorney general to bring an action to enforce the bill's requirements; and

5. deems violations a Connecticut Unfair Trade Practices Act (CUTPA) violation.

The bill's consumer data privacy requirements generally apply to individuals (1) conducting business in Connecticut or producing products or services targeted to Connecticut residents and (2) controlling or processing personal data above specified consumer thresholds.

The bill exempts (1) various entities, including state and local governments, nonprofits, and higher education institutions and (2)

specified information and data, including certain health records, identifiable private information for human research, certain credit-related information, and certain information collected under specified federal laws.

The bill also establishes a working group to, among other things, study Health Insurance Portability and Accountability Act (HIPAA)-adjacent data and other topics on data privacy, and make recommendations to the General Law Committee by January 1, 2023.

EFFECTIVE DATE: July 1, 2023, except the working group provision is effective upon passage.

§§ 1 & 2 — CONTROLLERS AND PROCESSORS SUBJECT TO THE BILL'S REQUIREMENTS

The bill's requirements generally apply to individuals and entities that do business in Connecticut or produce products or services targeting Connecticut residents and, during the preceding year, controlled or processed personal data of at least:

1. 75,000 consumers, excluding personal data controlled or processed solely for completing a payment transaction; or

2. 25,000 consumers and derived more than 25% of their gross revenue from selling personal data.

The bill defines a consumer as a state resident, but excludes an individual acting (1) in a commercial or employment context or (2) 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 person's role with the entity.

Under the bill, a "controller" is an individual or legal entity who, alone or jointly with others, determines the purpose and means of processing personal data. A "processor" is an individual or legal entity that processes personal data on a controller's behalf.

"Personal data" is any information that is linked, or reasonably linkable, to an identified or identifiable individual excluding de-identified data or publicly available information. "Publicly available information" means information that (1) is lawfully made available through federal, state, or municipal government records, or widely distributed media and (2) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

"Process" or "processing" means any manual or automatic operation or set of operations performed, on personal data or on sets of personal data, including collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data.

§ 3 — EXEMPTIONS

Entities

The bill does not apply to any:

1. state body, authority, board, bureau, commission, district, or agency or those of its political subdivisions;
2. federally tax exempt nonprofit organization;
3. private or public higher education institution;
4. certain national securities associations that are required to register under federal law;
5. financial institution or data subject to certain provisions of the Gramm Leach-Bliley Act (15 U.S.C. 6801 et seq.); or
6. nonprofit or for-profit hospital.

Information and Data

The bill also exempts the following information and data:

1. protected health information under HIPAA (42 U.S.C. 1320d et seq.);
2. patient identifying information for purposes of a federal

substance abuse and mental health law (42 U.S.C. 290dd-2);

3. identifiable private information for the purposes of the federal policy for protecting human subjects (45 C.F.R. Part 46);

4. identifiable private information that is collected as part of human subject research under the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;

5. information and data related to protecting human subjects (21 C.F.R. Parts 6, 50, and 56) or personal data used or shared in research that is conducted in accordance with the standards protecting human subjects the bill exempts above, or other research conducted in accordance with applicable law (45 C.F.R. 164.501);

6. information and documents created for the purposes of the Health Care Quality Improvement Act of 1986 (42 U.S.C. 11101 et seq.);

7. patient safety work product for the purposes of patient safety organizations under state law (CGS § 19a-127o) and the federal Patient Safety and Quality Improvement Act (42 U.S.C. 299b-21 et seq.);

8. information derived from any health care related information listed in the information or data exemption list that is de-identified according to HIPAA's de-identification requirements;

9. information originating from, and intermingled to be indistinguishable with, or treated in the same manner as other exempt information under the bill, maintained by a covered entity (e.g., health care providers and plans) or business associate, program, or qualified service organization, as specified in a federal law related to substance abuse and mental health (42 U.S.C. 290dd-2);

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

11. the collection, maintenance, disclosure, sale, communication, or use of any personal information relating to 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 activity is regulated by and authorized under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

12. personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.);

13. personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. 1232g et seq.);

14. personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. 2001 et seq.);

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 an individual's emergency contact information and used for these purposes; or (c) that is necessary to retain to administer benefits for another individual whose data is HIPAA-protected; and

16. personal data collected, processed, sold, or disclosed in relation to price, route, or service, as used in the federal Airline Deregulation Act (49 U.S.C. 40101 et seq.), by an air carrier subject

to the act, to the extent the bill is preempted by the Airline Deregulation Act (49 U.S.C. 41713).

Parental Consent Exemption

The bill deems controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act (COPPA) (15 U.S.C. 6501 et seq.) compliant with any obligation to obtain parental consent under the bill. Under the bill, COPPA includes the regulations, rules, guidance, and exemptions adopted under the act.

§ 4 — CONSUMER RIGHTS

With certain exceptions, the bill allows consumers to exercise the following rights:

1. confirm whether or not a controller is processing the consumer's personal data and access the data;

2. correct inaccuracies in the consumer's personal data, considering its nature and the reason it is being processed;

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

4. obtain a copy of the consumer's personal data processed by the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided the controller is not required to reveal any trade secret; and

5. opt out personal data processing for the purposes of "targeted advertising," the "sale of personal data," except as allowed under the bill for opting out of club programs (e.g., loyalty program § 6), or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer (i.e., controller decisions that result in providing or

denying financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services).

The bill defines "profiling" as 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.

Under the bill, "targeted advertising" means displaying specific advertisements to a consumer based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. It does not include:

1. advertisements based on activities within a controller's own websites or online applications;

2. advertisements based on the context of a consumer's current search query, visit to a website, or online application;

3. advertisements directed to a consumer in response to the consumer's request for information or feedback; or

4. processing personal data solely measuring or reporting advertising frequency, performance, or reach.

"Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. It excludes the following:

1. disclosing personal data (a) to a processor that processes the personal data on the controller's behalf, (b) to a third party for purposes of providing a product or service the consumer requested, or (c) where the consumer directs the controller to disclose the data or intentionally uses the controller to interact

with a third party;

2. disclosing or transferring personal data to (a) the controller's affiliate or (b) a third party as an asset that is part of an actual or proposed merger, acquisition, bankruptcy, or other transaction where the third party assumes control of all or part of the controller's assets;

3. disclosing personal data that the consumer (a) intentionally made available to the general public through mass media, and (b) did not restrict to a specific audience.

Controller's Response

Except as otherwise provided by the bill, a controller must comply with a consumer's request to exercise these rights.

The bill requires a controller to respond to the consumer without undue delay, but within 45 days after getting the request. The controller may extend the response period for 45 more days when reasonably necessary considering the complexity and number of the consumer's requests. The controller must tell the consumer about any extension within the initial response period and the reason for it.

If a controller declines to act on the consumer's request, the controller must tell the consumer without undue delay, but within 45 days after getting the request. The notice must include the justification for declining to act and instructions on how to appeal the decision.

Under the bill, a controller must give information in response to a consumer request for free, once per consumer during any 12-month period. If the consumer's request is 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 showing why the request was manifestly unfounded, excessive, or repetitive.

If a controller is unable to authenticate the request using

commercially reasonable efforts, the controller is not required to comply with the request to initiate an action under this provision. The controller must notify the consumer that it is unable to authenticate the request until the consumer provides more information reasonably necessary to authenticate the consumer and his or her request.

Under the bill, a controller that obtained personal data about a consumer from a source other than the consumer, is deemed in compliance with a consumer's request to delete the data if the controller:

1. retains a record of the deletion request and the minimum data needed for ensuring the consumer's personal data remains deleted from the business records and does not use the retained data for any other purpose pursuant to the bill's requirements, or

2. opts the consumer out of the processing of the personal data for any purposes, except those the bill exempts from its requirements.

The bill requires controllers to set up a process for a consumer to appeal the controller's refusal to act on a request within a reasonable time period after the consumer gets the decision. The appeals process must be conspicuously available and like the process for submitting requests to initiate action. Within 60 days after receiving an appeal, a controller must inform the consumer in writing of any action taken in response to the appeal, including a written explanation of the reasons for the decision. If the controller denies the appeal, it must also give the consumer a specified method for contacting the attorney general and submitting a complaint.

§§ 4 & 5 — CONSUMER'S AUTHORIZED AGENT

The bill allows a consumer to exercise certain rights under this provision by a secure and reliable means set by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent to exercise his or her right to opt out of the processing of his or her personal data for purposes of targeted advertising, the sale of personal data, or automatic profiling.

The consumer may designate the authorized agent using technology, such as an Internet link or browser setting, browser extension or global device setting, indicating the consumer's intent to opt out of the processing. The bill requires a controller to comply with an opt-out request from an authorized agent if the controller can authenticate, with commercially reasonable effort, the consumer's identity and the authorized agent's authority to act on the consumer's behalf.

Children and Individuals Subject to Protective Arrangements

In the case of processing a child's personal data, the bill allows a parent or legal guardian to exercise these 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 consumer's guardian or conservator may exercise these rights on the consumer's behalf.

§ 6 — CONTROLLERS

Requirements

The bill places many requirements on controllers. It requires them to:

1. limit the collection of personal data to what is adequate, relevant, and reasonably necessary for the purpose of data processing, as disclosed to the consumer;

2. establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue; and

3. offer an effective mechanism for a consumer to revoke his or her consent that is at least as easy as the mechanism the consumer used to give consent. When consent is revoked, the controller must stop processing the data as soon as practicable, but within 15 days of getting the request.

Prohibitions

Under the bill, controllers are also prohibited from processing:

1. personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer, except with the consumer's consent (i.e., a clear affirmative act signifying the consumer's informed agreement to allow the processing of their personal data, including by written statement, which may be electronic) or as allowed under the bill;

2. sensitive data about the consumer without their consent, or if the consumer is a known child (i.e., someone under age 13), without processing the data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.);

3. personal data in violation of state and federal law that prohibit unlawful discrimination against consumers; and

4. a consumer's personal data for targeted advertising or selling the data without the consumer's consent, where a controller has actual knowledge of, or willfully disregards, that the consumer is at least 13, but under 18, years of age.

Under the bill, a consumer's consent does not include (1) acceptance of a general or broad term of use or similar document that contains personal data processing descriptions along with other, unrelated information; (2) hovering over, muting, pausing, or closing a given piece of content; or (3) agreement obtained through the use of dark patterns. A "dark pattern" (1) is a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice and (2) includes any practice the Federal Trade Commission refers to as "dark pattern."

Under the bill, "sensitive data" means personal data that includes: (1) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status; (2) processing genetic or biometric

data in order to uniquely identify an individual; (3) personal data collected from a known child; or (4) precise geolocation data (i.e., information derived from technology).

Discrimination

The bill prohibits controllers from discriminating against a consumer for exercising any rights the bill allows. This includes denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

Goods or Services a Controller Does Not Collect

The bill specifies that a controller is not required to provide a product or service that requires a consumer's personal data that the controller does not collect or maintain.

Difference in Goods or Services (e.g., Club Program)

The bill allows controllers to offer 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 connected with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

If a consumer exercises his or her right to opt out of personal data processing, targeted advertising, or automatic profiling, a controller may not sell the consumer's personal data to a third party as part of the program unless:

1. the sale is reasonably necessary to enable the third party to provide a benefit the consumer is entitled to;

2. the sale of personal data to a third party is clearly disclosed in the program's terms; and

3. the third party uses the personal data only to facilitate the benefit the consumer is entitled to and does not keep, use, or disclose the data for any other purpose.

Privacy Notice and Disclosure

The bill requires controllers to provide consumers with a reasonably accessible, clear, and meaningful privacy notice. The notice must include:

1. the categories of personal data the controller processes;

2. the purpose for processing personal data;

3. how consumers may exercise their data privacy rights, including how a consumer may appeal a controller's decision about 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 e-mail address that the consumer can use to contract the controller.

Under the bill, if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose the processing, as well as how a consumer can exercise his or her opt-out rights.

The controller must set up, and describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise the consumer rights the bill allows. The means must consider how the consumer normally interacts with the controller, the need for secure and reliable communications for these requests, and the ability of the controller to authenticate the consumer's identity.

Under the bill, any of these means must include, providing a clear and conspicuous link on the controller's website to a website that enables a consumer or the consumer's agent to opt out of the targeted advertising or sale of the consumer's personal data.

By January 1, 2025, consumers must be allowed to opt out of any processing of the consumer's personal data for targeted advertising, or personal data sales. The opt-out preference must be sent, with the consumer's consent, by a platform, technology, or mechanism to the controller indicating the consumer's intent to opt-out of the processing or sale.

The bill requires the platform, technology, or mechanism to:

1. not unfairly disadvantage another controller;
2. not make use of a default setting, but instead require the consumer to affirmatively and freely give an unambiguous choice to opt out of any processing of his or her personal data that the bill regulates;
3. be consumer-friendly and easy to use by the average consumer;
4. be as consistent as possible with other similar platform, technology, or mechanisms required by federal or state law or regulation; and
5. enable the controller to accurately determine whether the consumer is a Connecticut resident and whether the consumer has made a legitimate request to opt out of any sale of his or her personal data or targeted advertising.

If a consumer's opt-out of targeted advertising or the sale of their personal data conflicts with his or her existing business-specific privacy setting or participation in a business's financial incentive program, the business must comply with the consumer's opt-out preference. The business may notify the consumer about the conflict and provide the consumer the choice to confirm the privacy setting or participation in the program.

If a controller responds to a consumer's opt-out request by informing the consumer of a charge for using any product or service, the controller must present the terms of any financial incentive offered for retaining,

using, selling, or sharing the consumer's personal data.

Under the bill, controllers must not require a consumer to create a new account in order to make a request, but can require them to use an existing account.

§ 7 — PROCESSORS

Controller's Instructions and Providing Assistance

The bill requires processors to adhere to the controller's instructions and assist the controller in meeting the controller's obligations under the bill. This assistance must consider the nature of processing and the information available to the processor and include:

1. appropriate technical and organizational measures, as reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests; and

2. 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 security breach of the processor's system under the state's existing data security law.

Processors must also provide necessary information to enable the controller to conduct and document data protection assessments.

Contracts

Under the bill, a contract between a controller and a processor must govern the processor's data processing procedures for processing performed on the controller's behalf. The contract must have clear instructions for processing data, the processing's nature, purpose, and duration, and both parties' rights and obligations.

The contract must also require the processor:

1. ensure that each person processing personal data is subject to a duty of confidentiality regarding the data;

2. at the controller's direction, delete or return all personal data to

the controller as requested at the end of providing services, unless the law requires that it be retained;

3. upon the controller's reasonable request, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations under the bill;

4. engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the processor's obligations regarding personal data; and

5. allow, and cooperate with, the controller or the controller's designated assessor to make reasonable assessments, or the processor may arrange for a qualified and independent assessor to evaluate the processor's policies and technical and organizational measures regarding the bill's requirements, using an appropriate and accepted control standard or framework and assessment procedure for these assessments. (In such a case, the processor must give a report of the assessment to the controller on request.)

The bill states that nothing in this provision should be construed to relieve a controller or a processor from the liabilities imposed on it based on its role in the processing relationship.

Fact-based Determination for Controller

Under the bill, determining whether a person is acting as a controller or processor for a specific data process is a fact-based determination that depends on the context in which the data is processed.

A person who is not limited in processing personal data under a controller's instructions, or who fails to adhere to these instructions, is a controller and not a processor with respect that specific processing of data. A processor that continues to adhere to a controller's instructions with a specific data processing remains a processor. If a processor begins, alone or with others, determining the purposes and means of the

processing of personal data, the processor is a controller with respect to that processing.

§ 8 — DATA PROTECTION ASSESSMENT

Assessment Requirements

The bill requires a controller to conduct and document a data protection assessment for each of the controller's processing activities that presents a heighted risk of harm to a consumer. This includes the: (1) processing personal data for targeted advertising purposes, (2) selling personal data, and (3) processing sensitive data.

Controllers must also conduct an assessment for processing personal data used for profiling, when the profiling presents a reasonably foreseeable risk of:

1. unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

2. financial, physical, or reputational injury to consumers;

3. a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where this intrusion would be offensive to a reasonable person; or

4. other substantial injury to consumers.

Under the bill, data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, consumer, other stakeholders, and the public against the potential risks to the consumer's rights associated with the processing, as mitigated by the controller's safeguards. They must also take into account the use of de-identified data (as described below) and the consumer's reasonable expectations, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

The bill allows the attorney general to require a controller to disclose and make available any data protection assessment relevant to his

investigations. The attorney general may evaluate the assessment for compliance with the responsibilities the bill imposes. The assessments are confidential and exempt from disclosure under the state's Freedom of Information Act. To the extent any information in an assessment disclosed to the attorney general includes information subject to attorney-client privilege or work product protection, the bill specifies that a disclosure does not constitute a waiver of the privilege or protection.

The bill allows a single data protection assessment to address a comparable set of processing operations that include similar activities. If a controller conducts an assessment to comply with another applicable law or regulation, that assessment is deemed to satisfy the bill's requirements if it is reasonably similar in scope and effect.

The bill specifies that data protection assessment requirements apply to processing activities created or generated after July 1, 2023, and are not retroactive.

§ 9 — DE-IDENTIFIED DATA

Requirements

The bill requires any controller that possesses de-identified data to:

1. take reasonable measures to ensure 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 recipient of the de-identified data to comply with the bill's requirements.

Under the bill, "de-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, a specific individual or their device. To be de-identified, a controller that possesses the data must (1) take reasonable measures to ensure the data cannot be associated with the individual, (2) publicly commits to

process the data only in a de-identified fashion and does not attempt to re-identify the data, and (3) contractually obligates anyone receiving the data to satisfy these requirements.

Applicability

The bill specifies that it should not be construed to (1) require a controller or processor to re-identify de-identified 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. Additionally, it does not 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.

Under the bill, an "authenticated" request is one made using reasonable means to determine that a request to exercise any of the rights afforded under the bill is being made by the consumer who is entitled to exercise these consumer rights with respect to the personal data at issue.

Pseudonymous Data

Under the bill, a consumer's rights under the bill specified above (see § 4) do not apply to pseudonymous data when the controller is able to demonstrate any information needed to identify the consumer is kept separately and has effective technical and organizational controls that

prevent the controller from accessing it.

The bill defines "pseudonymous data" as personal data that cannot be attributed to a specific individual without using additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

The bill requires a controller that discloses pseudonymous or de-identified data to exercise reasonable oversight to monitor compliance with any contractual commitments to which the data is subject. Controllers must take appropriate steps to address any such contractual breaches.

§ 10 — PROCESSING PERSONAL DATA FOR SPECIFIED PURPOSES

Ability to Comply With or Take Certain Other Actions

The bill specifies that nothing in its provisions should be construed to restrict a controller's or processor's ability to:

1. comply with federal, state, or municipal ordinances or regulations or a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other governmental authorities;

2. 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;

3. investigate, establish, exercise, prepare for, or defend legal claims;

4. provide a product or service a consumer specifically requested;

5. perform a contract to which a consumer is a party, including by fulfilling written warranty terms;

6. take steps at the consumer's request before entering into a contract;

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

8. 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;

9. engage in public- or peer-reviewed scientific or statistical research in the public interest that follows applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities, that determine if (a) deleting the information is likely to provide substantial benefits that do not exclusively benefit the controller, (b) the research's expected benefits outweigh the privacy risk, (c) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

10. assist another controller, processor, or third party with any obligations under the bill; or

11. process personal data for public interest reasons in public health, community health, or population health, but solely to the extent that the processing is (a) subject to suitable and specific measures to safeguard the consumer's rights whose personal data is being processed, and (b) under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

Ability to Collect, Use, or Retain Data. The bill also specifies that

the obligations it imposes on controllers or processors do not restrict their 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. recall products;

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

4. perform internal operations that are reasonably aligned with the consumer's expectations, reasonably anticipated based on the consumer's existing relationship with the controller, or compatible with processing data based on (a) providing a product or service the consumer specifically requested or (b) performing a contract to which the consumer is a party.

Evidentiary Privilege. Under the bill, the obligations imposed on controllers or processors do not apply if doing so would make them violate state evidentiary privilege. The bill should not be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by state evidentiary privilege laws as a privileged communication.

Third-Party Liability. Under the bill, controllers or processors that disclose personal data to a third party in compliance with the bill's requirements are not responsible for violations by them.

At the time of disclosure, the original controllers or processors must not have had reason to believe that the recipient would violate the bill. A third party controller or processor receiving personal data from a controller or processor in compliance with the bill is also not in violation for the controller's or processor's transgressions.

First Amendment Rights. The bill states that its provisions are not an obligation imposed on controllers and processors that adversely affects any individual's rights or freedoms, such as exercising the right

of free speech under the First Amendment of the U.S. Constitution. It also does not affect a person processing personal data for a purely personal or household activity.

Limitations on Processing Personal Data. Under the bill, controllers may process data to the extent the processing is (1) reasonably necessary and proportionate to the purposes listed above (e.g., for internal research or effectuate product recall) and (2) adequate, relevant, and limited to what is necessary to the specific listed purpose. When applicable, personal data collected, used, or retained must consider the nature and purposes of these actions. The data must be subject to reasonable administrative, technical, and physical measures to protect its confidentiality, integrity, and accessibility and to reduce reasonably foreseeable risks of harm to consumers related to its collection, use, or retention.

Under the bill, if a controller processes personal data for a specified purpose through one of the exemptions listed above, the controller bears the burden of showing that the processing (1) qualifies for an exemption under the bill and (2) complies with the bill's requirements for processing personal data.

The bill specifies that processing personal data for the purposes expressly identified in this provision does not, on its own, make an entity a controller.

§ 11 — ATTORNEY GENERAL POWERS

Exclusive Authority

Under the bill and with certain exceptions, the attorney general has exclusive authority to enforce the bill's provisions. The bill establishes a grace period through December 31, 2024, during which the attorney general must give violators an opportunity to cure any violations. Beginning January 1, 2025, the bill appears to allow the attorney general to enforce these provisions without requiring him to provide notice and an opportunity for correction.

The bill specifies that none of its provisions should be construed as

providing the basis for, or be subject to, a private right of action for violations under the bill or any other law.

Under the bill, any violation of the bill's requirements is an unfair trade practices violation (CUTPA) and is enforced solely by the attorney general, provided CUTPA's private right of action and class action provisions do not apply to the violation.

Notice and Opportunity to Correct Violations

From July 1, 2023, to December 31, 2024, the bill requires the attorney general to, before initiating any action for a violation of the bill's provisions, issue a notice of violation to the controller if he determines a cure is possible. If the controller fails to cure the violation within 60 days of receiving notice, the attorney general may bring an action.

Under the bill, by February 1, 2024, the attorney general must submit a report to the General Law Committee disclosing:

1. the number of notices of violations he issued,
2. the nature of each violation,
3. the number of violations cured within the 60-day period, and
4. any other matters he deems relevant.

Violations After January 1, 2025

Beginning on January 1, 2025, the attorney general may, in determining whether to allow a controller or processor the opportunity to cure an alleged violation, consider (1) the number of violations, (2) the controller's or processor's size and complexity and the nature and extent of the controller's or processor's processing activities, (3) the substantial likelihood of injury to the public, and (4) the safety of individuals or property.

§ 12 — WORKING GROUP

By September 1, 2022, the bill requires the General Law Committee chairpersons to convene a working group to study:

1. how HIPAA-adjacent data is handled and recommend legislation, if any, needed to ensure the protection of this data;

2. algorithmic decision-making and make recommendations concerning the proper use of data to reduce bias in this decision-making; and

3. other data privacy topics.

The General Law chairpersons must serve as the working group's chairpersons and jointly appoint its members. The members must include representatives from the industry, academia, consumer advocacy groups, small and large companies, the attorney general's office, and attorneys with privacy law expertise. The General Law Committee's administrative staff must serve as the working group's administrative staff.

By January 1, 2023, the bill requires the working group to submit a report on its findings and recommendations to the General Law Committee. And it terminates on the date it submits the report or January 1, 2023, whichever is later.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 14 Nay 4 (03/15/2022)