General Assembly

Substitute Bill No. 893

January Session, 2021

* SB00893GL 032321 *

AN ACT CONCERNING CONSUMER PRIVACY.

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

Section 1. (NEW) (*Effective January 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 controls, is controlled by, or is under common control with another legal entity or shares common branding 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 verify through reasonable means that the consumer is the same consumer exercising 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, voiceprint, eye retinas, irises or other unique biological

patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used or stored for health care treatment, payment or operations under HIPAA.

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

(5) "Child" means any natural person less than thirteen years of age.

(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.

(7) "Consumer" means a natural person who is a resident of this state and acting only in an individual or household context. "Consumer" does not include a natural person acting in a commercial or employment context.

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

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

(10) "Decisions that produce legal or similarly significant effects concerning a consumer" means decisions made by the controller that result in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services or access to basic necessities, such as food and water.

(11) "De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person.

(12) "Health record" means the health-related record of an individual, and may include, but need not be limited to, continuity of care documents, discharge summaries and other information or data relating to a patient's demographics, medical history, medication, allergies, immunizations, laboratory test results, radiology or other diagnostic images, vital signs and statistics.

(13) "Health care provider" means any person, corporation, limited liability company, facility or institution licensed by this state to provide health care or professional services, or an officer, employee or agent thereof acting in the course and scope of his or her employment.

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

(15) "Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly.

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

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

(18) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "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 identify the specific location of a natural person 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 a natural 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 natural person'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 natural person without the use of additional information, provided that 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 natural person.

(25) "Publicly available information" means information that is lawfully made available through federal, state or municipal government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

(26) "Sale of personal data" means the exchange of personal data for monetary 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 information 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 (E) 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 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 diagnosis, sexual orientation or citizenship or immigration status, (B) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person, (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 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) the processing of personal data solely for measuring or reporting advertising performance, reach or frequency.

(29) "Third party" means a natural or legal person, public authority, agency or body other than the consumer, controller, processor or an

affiliate of the processor or the controller.

Sec. 2. (NEW) (*Effective January 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: (1) During a calendar year, control or process the personal data of not less than one hundred thousand consumers, or (2) control or process the personal data of not less than twenty-five thousand consumers and derive more than fifty per cent of their gross revenue from the sale of personal data.

Sec. 3. (NEW) (*Effective January 1, 2023*) (a) The provisions of sections 1 to 11, inclusive, of this act shall not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state, (2) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., (3) covered entity or business associate governed by the privacy, security and breach notification rules issued by the United States Department of Health and Human Services, 45 CFR 160 and 164, established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act, (4) nonprofit organization, or (5) institution of higher education.

(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) health records, (3) patient identifying information for purposes of 42 USC 290dd-2, (4) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46, (5) 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, (6) the protection of human subjects under 21 CFR 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 (4) and (5) of this subsection, or other

research conducted in accordance with applicable law, (7) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq., (8) patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., (9) 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, (10) 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, (11) information used for public health activities and purposes as authorized by HIPAA, (12) 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., (13) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., (14) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., (15) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., and (16) 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 under subdivision (1) of this subsection and used for the purposes of administering such

benefits.

(c) Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act, 15 USC 6501 et seq., 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 January 1, 2023*) (a) A consumer may invoke the consumer rights authorized pursuant to this section at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing personal data belonging to the known child. A controller shall comply with an authenticated consumer request to exercise the right to: (1) Confirm whether or not a controller is processing the consumer's personal data and to access such personal data, (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data, (3) delete personal data provided by, or obtained about, the consumer, (4) obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, and (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, or (C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(b) 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

response period may be extended once by forty-five additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial forty-five-day response period, together with the reason for the extension.

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

(3) Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(c) 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 January 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 the federal Children's Online Privacy Protection Act, 15 USC 6501 et seq., and (5) not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 1 to 11, inclusive, of this act, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods and services to the consumer. Nothing in this subsection shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to 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 consumer has exercised his right to opt out or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.

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

(c) 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.

(d) 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. Controllers 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.

Sec. 6. (NEW) (*Effective January 1, 2023*) (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations pursuant to 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 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 include requirements that the processor shall: (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 a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined 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 processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

Sec. 7. (NEW) (*Effective January 1, 2023*) (a) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data: (1) The processing of personal data for purposes of targeted advertising, (2) the sale of personal data, (3) the processing of personal data for 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, (4) the processing of sensitive data, and (5) any processing activities involving personal data that present a heightened risk of harm to consumers.

(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 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, shall be factored into this assessment by the controller.

(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. The disclosure of a data protection assessment pursuant to a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

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

(e) Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

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

Sec. 8. (NEW) (*Effective January 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 a natural person, (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 all of the following are true, if the controller: (1) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data, (2) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer, and (3) does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(d) Consumer rights shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

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

Sec. 9. (NEW) (*Effective January 1, 2023*) (a) Nothing in sections 1 to 11, inclusive, of this act shall be construed to restrict a controller's or processor's ability to: (1) Comply with federal, state or municipal ordinances or regulations, (2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities, (3) cooperate with law-enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal,

state or municipal ordinances or regulations, (4) investigate, establish, exercise, prepare for or defend legal claims, (5) provide a product or service specifically requested by a consumer, (6) perform a contract to which a consumer is a party, including fulfilling the terms of a written warranty, (7) take steps at the request of a consumer prior to entering into a contract, (8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis, (9) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action, (10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board, or similar independent oversight entities that determine (A) if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller, (B) the expected benefits of the research outweigh the privacy risks, and (C) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification, or (11) assist another controller, processor, or third party with any of the obligations under sections 1 to 11, inclusive, of this act.

(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 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 actual knowledge that the recipient intended to commit a violation of 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 it 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 of free speech pursuant to 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 sections 1 to 11, inclusive, of this act shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by sections 1 to 11, inclusive, of this act. 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 an entity a controller with respect to such processing.

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

(b) Prior to initiating any action under sections 1 to 11, inclusive, of this act, the Attorney General shall provide a controller or processor not less than thirty days' written notice identifying the specific provisions of said sections the Attorney General, on behalf of a consumer, alleges have been or are being violated. If, prior to the expiration of such time period, the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action for statutory damages shall be initiated against the controller or processor.

(c) If a controller or processor continues to violate sections 1 to 11, inclusive, of this act in breach of an express written statement provided to the consumer under this section, the Attorney General may initiate a civil action in Superior Court and seek damages not exceeding seven thousand five hundred dollars for each violation of sections 1 to 11, inclusive, of this act.

(d) Nothing in sections 1 to 11, 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.

Sec. 11. (NEW) (*Effective January 1, 2023*) (a) The Attorney General shall have exclusive authority to enforce sections 1 to 10, inclusive, of this act by bringing an action in the name of the state, or on behalf of persons residing in this state.

(b) Any controller or processor that violates sections 1 to 10, inclusive, of this act shall be liable for a civil penalty of not more than seven thousand five hundred dollars for each violation.

(c) The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, of any action initiated under sections 1 to 10, inclusive, of this act.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*January 1, 2023*	New section
Sec. 2	*January 1, 2023*	New section
Sec. 3	*January 1, 2023*	New section
Sec. 4	*January 1, 2023*	New section
Sec. 5	*January 1, 2023*	New section
Sec. 6	*January 1, 2023*	New section
Sec. 7	*January 1, 2023*	New section
Sec. 8	*January 1, 2023*	New section
Sec. 9	*January 1, 2023*	New section
Sec. 10	*January 1, 2023*	New section
Sec. 11	*January 1, 2023*	New section

Statement of Legislative Commissioners:
In Sec. 10(b), the words "the expiration of" were inserted in the second sentence for clarity and consistency.

GL *Joint Favorable Subst.*