HOUSE . . . . . No. 4514

The Commonwealth of Massachusetts

HOUSE OF REPRESENTATIVES, March 3, 2022.

The committee on Advanced Information Technology, the Internet and Cybersecurity to whom was referred the petition (accompanied by bill, House, No. 142) of Andres X. Vargas, David M. Rogers and others relative to consumer data privacy, reports recommending that the accompanying bill (House, No. 4514) ought to pass.

For the committee,

LINDA DEAN CAMPBELL.

FILED ON: 2/1/2022

HOUSE . . . . . No. 4514

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Second General Court
(2021-2022)

An Act establishing the Massachusetts Information Privacy and Security Act..

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws are hereby amended by inserting after Chapter 93L the following chapter:

CHAPTER 93M. The Massachusetts Information Privacy and Security Act.

SECTION 1. Title

This chapter shall be known as the "Massachusetts Information Privacy and Security Act."

SECTION 2. Definitions

As used in this chapter, the following words shall have the following meanings unless the context clearly requires otherwise:

"Advertising" means a communication in any medium by a controller or an entity acting on the controller's behalf intended to induce an individual to obtain goods, services, or employment.

"Affiliate" means an entity that controls, is controlled by, or is under common control or shares common branding with another entity. For the purposes of this definition, "control" or "controlled" shall mean: (1) ownership of more than fifty per cent of the outstanding shares of any class of voting security of the entity; (2) control in any manner over the election of a majority of the entity's directors or of persons exercising similar functions; or (3) the power to otherwise exercise a controlling influence over the management of the entity.

"Authorized agent" means an entity or natural person that an individual has designated pursuant to subsection (d) of section 15 of this chapter.

"Biometric information" means a retina or iris scan, fingerprint, voiceprint, map or scan of hand or face geometry, vein patterns, gait patterns, or other measurements of unique biological patterns or characteristics used to identify a specific individual; provided, however, that "biometric information" shall not include: (i) writing samples; (ii) written signatures; (iii) photographs; (iv) video or audio recordings or data generated therefrom; (v) human biological samples used for valid scientific testing or screening; (vi) demographic data; (vii) tattoo descriptions; (viii) physical descriptions such as height, weight, hair color or eye color; (ix) donated organs, tissues, or parts as defined in chapter 113A of the General Laws; (x) blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency; (xi) biological materials regulated under section 70G of chapter 111 of the General Laws; (xii) information captured from a patient in a health care setting; (xiii) information collected, used, or stored for health care treatment, payment or operations under HIPAA; or (xiv) an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used

to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Business associate" shall have the same meaning as in 45 C.F.R. 160.103.

"Child" means an individual who a controller knows or reasonably should know is under the age of 13.

"Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or otherwise accessing any personal information pertaining to an individual by any means. This includes, but is not limited to, obtaining information from the individual, either actively or passively, or by observing the individual's behavior.

"Common branding" means a shared name, servicemark, trademark, or other indicator that an individual would reasonably understand to indicate that two or more entities are commonly owned.

"Consent" means a clear affirmative act signifying an individual's freely given, specific, informed, and unambiguous agreement to allow the processing of personal information relating to the individual for a narrowly defined particular purpose. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. The following shall not constitute consent: (1) acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information; (2) hovering over, muting, pausing, or closing a given piece of content; or (3) agreement obtained through dark patterns.

"Controller" means the entity that, alone or jointly with others, determines the purposes and means of the processing of personal information of an individual.

"Covered entity" shall have the same meaning as in 45 C.F.R. 160.103.

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

"Data broker" means a controller that knowingly collects and sells to third parties:

(1) The sensitive information of not less than 10,000 individuals; or

(2) The personal information of not less than 10,000 individuals with whom the controller does not have a direct relationship, including, but not limited to, a relationship in which an individual is a past or present: (i) customer, client, subscriber, user, or registered user of the controller's goods or services; (ii) an employee, contractor, or agent of the controller; (iii) an investor in the controller; or (iv) a donor to the controller.

The following activities conducted by a controller, and the collection and sale of personal information incidental to conducting these activities, shall not qualify the controller as a data broker: (i) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier; (ii) providing publicly available information related to an individual's business or profession; or (iii) providing publicly available information via real-time or near-real-time alert services for health or safety purposes.

"De-identified information" means information, derived from personal information, that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or

identifiable individual or household, or a device linked to such individual or household. De-identification means the creation of de-identified information from personal information.

"Designated methods for submitting a request" means a mailing address, email address, Internet web page, Internet web portal, toll-free telephone number, or other applicable contact information, whereby an individual may submit a request or direction under this chapter, provided that: (1) the designated methods shall be reasonably accessible to individuals and take into account the ways in which individuals interact with the controller, the need for secure and reliable communication of the request, and the ability of the controller to determine that the request is a verifiable request; and (2) a controller shall not require an individual to create a new account in order to exercise a right under this chapter, but a controller may require an individual to use an existing account to exercise the individual's rights under this chapter.

"Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

"Entity" means a sole proprietorship, or a corporation, association, partnership or other legal entity.

"Health care facility" shall have the same meaning as defined in section 25B of chapter 111 of the General Laws.

"Health care provider" shall have the same meaning as defined in section 1 of chapter 111 of the General Laws.

"Health record" means an individual's health-related record, as kept pursuant to section 70 of chapter 111 of the General Laws.

"HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq., as amended from time to time.

"Homepage" means the introductory page of an Internet website and any Internet web page where personal information is collected; provided, however, that in the case of an online service, such as a mobile application, homepage shall mean: (i) the application's platform page or download page; (ii) a link within the application, such as from the application configuration, "About," "Information," or settings page; or (iii) any other location that allows individuals to review the notices required by this chapter, including, but not limited to, before downloading the application.

"Identified or identifiable individual household" is a group of individuals who: (i) cohabitate with one another at the same residential address in the Commonwealth; (ii) use common devices or services; and (iii) can be readily identified, directly or indirectly.

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

"Individual" means a natural person who is a resident of the Commonwealth; provided, however, that "individual" shall not include a natural person acting as a sole proprietorship.

"Infer" or "inference" means the derivation of information, data, assumptions or conclusions from facts, evidence, or another source of information or data.

"Institution of higher education" means any college, junior college, university or other public or private educational institution that has been authorized to grant degrees pursuant to sections 30, 30A, and 31A of chapter 69 of the General Laws.

"Intentionally interacts" means when an individual intends to interact with an entity, or disclose personal information to an entity, via one or more deliberate interactions, including visiting the entity's website or purchasing a good or service from the entity; provided, however, that hovering over, muting, pausing, or closing a given piece of content does not constitute an individual's intent to interact with an entity.

"Minor" means an individual who a controller knows or reasonably should know is not less than 13 years of age and not more than 16 years of age.

"Nonpersonalized advertising" means advertising that is based solely on an individual's personal information, except for the individual's specific geolocation information, derived from the individual's current interaction with the controller.

"Nonprofit organization" means any organization that is exempt from taxation under 26 U.S.C. 501(c), as amended from time to time.

"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable individual; provided, however, that personal information shall not include de-identified information or publicly available information.

For the following purposes, personal information shall also include information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable household:

(1) As "personal information" is used in the definition of "sale," "sell" or "sold" in this section;

(2) In any other reference to the sale of personal information in this chapter; or

(3) As "personal information" is used in subsection (b) of section 3 of this chapter.

"Process" or "processing" means any operation or set of operations which are performed on personal information or on sets of personal information, whether or not by automated means, such as the collection, use, storage, disclosure, analysis, prediction, deletion, or modification of personal information. Process or processing includes the actions of a controller directing a processor to process personal information.

"Processor" means an entity that processes personal information on behalf of a controller.

"Protected health information" shall have the same meaning as defined in 45 C.F.R. 160.103, established pursuant to HIPAA.

"Publicly available information" means information about an individual that is: (1) lawfully made available from federal, state, or local government records; or (2) information that a controller has a reasonable basis to believe is lawfully and intentionally made available by the individual to the general public through widely distributed media.

"Research" means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge and that is conducted in accordance with other applicable ethics and privacy laws.

"Sale, "sell," or "sold" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, an individual's personal information by the controller to a third party for monetary

or other valuable consideration in a bargained-for exchange, or for the purposes of targeted advertising. "Sale," "sell," or "sold" does not include the following:

(1) The disclosure of personal information to a processor where the processor only processes such personal information on behalf of the controller;

(2) The controller's use or sharing of an identifier for an individual who has opted out of the sale of the individual's personal information or limited the use of the individual's sensitive information for the purposes of alerting entities that the individual has opted out of the sale of the individual's personal information or limited the use of the individual's sensitive information;

(3) The disclosure or transfer of personal information to an affiliate of the controller;

(4) The disclosure or transfer of personal information to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets;

(5) The disclosure of personal information to a third party for purposes of providing a product or service specifically requested by the individual; or

(6) When the individual uses or expressly directs the controller to disclose personal information to a third party or otherwise interact with a third party, not including disclosures or interactions for the purposes of targeted advertising; provided, however, that the individual's direction was not obtained through dark patterns.

"Security and integrity" means the ability of:

(1) Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information;

(2) Controllers to detect security incidents, resist malicious, deceptive, fraudulent or illegal actions and to help prosecute those responsible for those actions; or

(3) Controllers to ensure the physical safety of natural persons.

"Sensitive information" means:

(1) Personal information that reveals an individual's: (i) racial or ethnic origin, (ii) religious beliefs; or (iii) citizenship or immigration status;

(2) Biometric information or genetic information processed for the purpose of uniquely identifying an individual;

(3) Personal information processed concerning an individual's mental or physical health diagnosis or treatment;

(4) Personal information processed concerning an individual's sex life or sexual orientation;

(5) An individual's specific geolocation information;

(6) The personal information from a child;

(7) Personal information that reveals an individual's philosophical beliefs or union membership; or

(8) Personal information that reveals: (i) an individual's social security number, driver's license number, military identification number, passport number, or state-issued identification card number; or (ii) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account.

Sensitive information is a form of personal information. Sensitive information that is "publicly available information" shall not be considered sensitive information or personal information.

"Specific geolocation information" 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 an individual within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet. Specific geolocation information excludes the content of communications or any information generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

"Targeted advertising" means the targeting of advertising to an individual based on the individual's personal information obtained from the individual's activity across controllers, distinctly-branded websites, applications, or services, other than the controller, distinctly-branded website, application, or service with which the individual intentionally interacts. Targeted advertising shall not include:

(1) Advertising to an individual in response to the individual's request for information and feedback;

(2) Advertising based on the context of an individual's current search query, visit to a website, or online application; or

(3) Processing personal information solely for measuring or reporting advertising performance, reach, or frequency.

"Third party" means a natural person, entity, public authority, agency, or body other than the applicable individual, controller, processor, or affiliate of the controller or the processor.

"Verifiable request" means a request: (i) to exercise any of the rights set forth in sections 8 through 11 of this chapter; and (ii) that a controller can use commercially reasonable means to determine is being made by the individual or by a person authorized to exercise rights on behalf of such individual with respect to the personal information at issue, pursuant to subsections (b) and (c) of section 15 of this chapter.

SECTION 3. Scope and Applicability

(a) This chapter shall apply to:

(1) A controller or processor that conducts business in the Commonwealth; and

(2) The processing of personal information by a controller or processor not physically established in the Commonwealth, where the processing activities are related to: (i) the offering of goods or services that are targeted to individuals; or (ii) the monitoring of behavior of individuals where such behavior takes place in the Commonwealth.

(b) Notwithstanding subsection (a) of this section, sections 7 through 17 and section 20 of this chapter shall only apply to a controller that satisfies at least 1 of the following additional thresholds or is an entity that is an affiliate of and shares common branding with such a

controller, in which case sections 7 through 17 and section 20 shall apply only to the personal information processed by the affiliate on behalf of the controller:

(1) The controller, as of January 1 of the calendar year, had annual global gross revenues in excess of 25,000,000 dollars in the preceding calendar year;

(2) The controller determines the purposes and means of processing of the personal information of not less than 100,000 individuals; or

(3) The controller is a data broker.

(c) Payment-only credit, check, or cash transactions where no information is retained about an individual entering into the transaction do not count as "individuals" for the purposes of subsection (b).

(d) The provisions of this chapter are not limited to personal information collected electronically or over the Internet, but apply to the processing of all personal information processed by a controller.

(e) This chapter shall not apply to:

(1) Any agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

(2) Any national securities association that is registered under 15 U.S.C. 78o-3 of the Securities Exchange Act of 1934, as amended from time to time.

(3) Any registered futures association that is so designated pursuant to 7 U.S.C. 21, as amended from time to time.

(f) The following information shall be exempt from the provisions of this chapter:

(1) Protected health information that is processed by a covered entity or business associate pursuant to 45 C.F.R. 160, 162, and 164.

(2) Health records for the purposes of section 70 of chapter 111 of the General Laws, to the extent that the records are maintained pursuant to 45 C.F.R. 160, 162, and 164.

(3) Information and documents that are created by a covered entity for purposes of complying with HIPAA and its implementing regulations.

(4) Information used only for public health activities and purposes as authorized by HIPAA.

(5) Patient identifying information for purposes of 42 C.F.R. 2, established pursuant to 42 U.S.C. 290dd-2, as amended from time to time.

(6) Information that is: (i) collected for a clinical trial subject to the Federal Policy for the Protection of Human Subjects (also known as the Common Rule) under 45 C.F.R. 46; (ii) collected pursuant to good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; (iii) collected pursuant to the human subject protection requirements under 21 C.F.R. 50 and 56; or (iv) personal information used or disclosed in research conducted in accordance with one or more of the requirements set forth in this paragraph.

(7) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq., as amended from time to time.

(8) Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act, 42 U.S.C. 299b-21 et seq., as amended from time to time.

(9) Information that is: (i) derived from any of the health care-related information listed in this subsection; and (ii) de-identified in accordance with the requirements for de-identification pursuant to 45 C.F.R. 164.

(10) Information that is treated in the same manner as, or that originates from and is intermingled to be indistinguishable with, information exempt under this subsection that is maintained by: (i) a covered entity or business associate; (ii) a health care facility or health care provider; or (iii) a program of a qualified service organization as defined by 42 U.S.C. 290dd-2.

(11) (i) An activity involving the processing of any personal information bearing on an individual's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by: (A) a consumer reporting agency, as defined in 15 U.S.C. 1681a(f); (B) a furnisher of information, as set forth in 15 U.S.C. 1681s-2, that provides information for use in a consumer report, as defined in 15 U.S.C. 1681a(d); and (C) a user of a consumer report, as set forth in 15 U.S.C. 1681b.

(ii) Clause (i) of this paragraph shall apply only to the extent that: (A) the activity is regulated by the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq., as amended from time to time; and (B) the personal information is processed solely as authorized by the federal Fair Credit Reporting Act.

(12) Personal information processed in compliance with the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq. as amended from time to time, and implementing regulations.

(13) Personal information regulated by the federal Family Educational Rights and Privacy Act, 20 U.S.C. 1232g et seq. as amended from time to time, and its implementing regulations.

(14) Personal information processed in compliance with the federal Farm Credit Act, 12 U.S.C. 2001 et seq. as amended from time to time, and its implementing regulations, 12 C.F.R. 600 et seq.

(15) Personal information processed in compliance with the federal Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq. as amended from time to time, and its implementing regulations.

(16) Personal information processed in compliance with chapter 175I of the General Laws.

(17) Personal information processed in relation to price, route or service, as such terms are used in the Airline Deregulation Act, 49 U.S.C. 40101 et seq. as amended from time to time, by an air carrier subject to said act, to the extent that this chapter is preempted by section 41713 of the Airline Deregulation Act.

(18) Personal information processed for purposes of chapter 176Q of the General Laws.

(g) Sections 8 through 11 and section 13 of this chapter shall not apply to information that is processed: (1) in the course of an individual acting in a commercial context, to the extent that the information is collected and used within that context; (2) in the course of an individual acting as a job applicant to, an employee of, or an agent or independent contractor of a controller, processor, or third party, to the extent that the information is collected and used within the context of that role; (3) as the emergency contact information of an individual under paragraph

(2), provided that the information is used solely for emergency contact purposes; or (4) in order to administer benefits for another natural person relating to the individual under paragraph (2), provided that the information is used solely for the purposes of administering those benefits.

(h) The provisions of this chapter relating to individuals under 16 years of age shall only apply to the extent not in conflict with the federal Children's Online Privacy Protection Act, 15 U.S.C. 6501 et seq., and its implementing regulations. Controllers and processors that comply with the Children's Online Privacy Protection Act and its implementing regulations shall be in compliance with any obligation to obtain parental consent under this chapter.

(i) This chapter shall also apply in full to an entity that voluntarily certifies to the Attorney General that it is in compliance with, and agrees to be bound by, this chapter; provided, however, that the entity processes the personal information of one or more individuals but does not meet the applicability criteria set forth in subsection (b) of this section.

SECTION 4. Conflicting Provisions

Wherever possible, law relating to individuals' personal information should be construed to harmonize with the provisions of this chapter, but in the event of a conflict between the provisions of other laws and the provisions of this chapter, the provisions that afford the greatest protection for the right of privacy for individuals shall control.

SECTION 5. General Principles for Processing Personal Information

(a) Personal information shall be:

(1) Processed lawfully, fairly, and in a transparent manner in relation to the individual and in compliance with this chapter;

(2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(3) Processed in a manner that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

(4) Maintained in a manner such that the information is accurate and, where necessary, kept up to date;

(5) Maintained in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal information is processed; and

(6) Processed in a manner that ensures that the information remains appropriately secure.

(b) A controller shall be responsible for, and capable of demonstrating compliance with, the above subsection (a), including by implementing procedures to comply with the subsection that are reasonable and appropriate taking into consideration:

(1) The size, scope, and type of the controller;

(2) The amount of resources available to the controller;

(3) The amount and nature of personal information processed by the controller, including, but not limited to, whether the personal information is sensitive information; and

(4) The need for the security and confidentiality of the personal information processed by the controller.

(c) A controller that is compliant with the regulations promulgated pursuant to chapter 93H of the General Laws with respect to “personal information,” as that term is defined in

section 1 of said chapter 93H, shall be in compliance with the principle set forth in paragraph (6) of subsection (a) of this section with respect to such personal information.

SECTION 6. Lawful Bases For Processing Personal Information

(a) Processing shall be lawful and in compliance with this chapter only if and to the extent that at least 1 of the following applies:

(1) The individual has given consent to the processing of their personal information for one or more specific purposes;

(2) Processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;

(3) Processing is necessary for compliance with a legal obligation to which the controller is subject;

(4) Processing is necessary in order to protect the vital interests of the individual or of another natural person; provided, however, that the processing cannot be manifestly based on another legal basis and that the individual or other natural person is at risk or danger of death or serious physical injury; or

(5) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the individual's reasonable expectations of privacy or other legal rights.

(b) Processing pursuant to paragraph (5) of subsection (a) shall be consistent with the reasonable expectations of the individual based on the individual's relationship with the controller, and such processing shall be conspicuously disclosed to the individual in advance;

provided, however, that the controller shall also assess the following factors to determine whether there is a legitimate interest for the processing:

(1) The possible consequences and cognizable harms for the individual whose personal information would be processed;

(2) The amount and nature of personal information that would be processed;

(3) The need for the security and confidentiality of the personal information that would be processed;

(4) The context in which the personal information would be collected; and

(5) Whether the processing is necessary and proportionate in relation to the purposes, or whether the controller or third party can achieve their legitimate interests in another less intrusive way.

(c) A controller shall not rely on paragraph (5) of subsection (a) as a lawful basis for processing sensitive information unless the controller meets a heightened standard of proof, under which a controller shall conduct a documented risk assessment in accordance with section 21 of this chapter that shows that the legitimate interests pursued by the controller or by a third party substantially outweigh the individual's reasonable expectations of privacy or other legal rights. In particular, a controller shall not rely on paragraph (5) of subsection (a) to sell sensitive information that meets any of the subcategories set forth in paragraphs (1) through (5) in the definition of sensitive information in section 2 of this chapter.

(d) A controller shall not sell the personal information of a child unless the controller has obtained the consent of the parent or guardian of the child.

(e) A controller shall not sell the personal information of a minor unless the controller has obtained the minor's consent.

(f) If a minor does not consent to the sale of the minor's personal information, a controller shall: (1) wait for not less than 12 months before making a subsequent request for the minor's consent to sell the minor's personal information; or (2) wait until the individual attains 16 years of age, whichever occurs sooner.

SECTION 7. Right to Privacy Notice

(a) At or before the point of the collection of an individual's personal information, controllers shall provide the individual with a reasonably accessible, clear, and meaningful privacy notice that shall include:

(1) A clear and conspicuous description of: (i) whether the controller sells personal information to third parties or processes personal information for the purposes of targeted advertising; (ii) what categories of sensitive information, if any, the controller processes and for what purposes; (iii) an individual's rights pursuant to sections 8 through 13 of this chapter; (iv) how and where individuals may request to exercise these rights, pursuant to section 16 of this chapter; and (v) a link to the Attorney General's online mechanism through which the individual may contact the Attorney General to submit a complaint, pursuant to section 25 of this chapter.

(2) The categories of personal information processed by the controller;

(3) The controller's purposes for processing the personal information;

(4) The categories of personal information that the controller sells to third parties, specifying the categories of sensitive information that the controller sells to third parties, if any;

(5) The categories of third parties, if any, to whom the controller sells personal information;

(6) A contact method, such as an email address, that the individual may use to contact the controller; and

(7) The length of time the controller intends to retain each category of personal information, or if that is not possible, the criteria used to determine such period, provided that a controller shall retain personal information for a duration consistent with paragraph (5) of subsection (a) of section 5 of this chapter.

(b) A controller shall not collect additional categories of personal information or process personal information collected for additional purposes that are incompatible with the disclosed purposes for which the personal information was collected, without providing the individual with notice consistent with subsection (a) of this section.

(c) An entity that, acting as a third party, controls the collection of an individual's personal information may satisfy its obligation under this section by providing the required information prominently and conspicuously on the homepage of its Internet website; provided, however, that if an entity, acting as a third party, controls the collection of personal information about an individual on its premises, including in a vehicle, then the entity shall, at or before the point of collection, satisfy its obligation under subsection (a) of this section by providing the required information in a clear and conspicuous manner at such location.

(d) Nothing in this section shall require a controller to provide the information required in a manner that would disclose the controller's trade secrets.

(e) The categories of sensitive information required to be disclosed by a controller pursuant to this section shall specifically include each applicable subcategory set forth in paragraphs (1) through (8) in the definition of sensitive information in section 2 of this chapter.

SECTION 8. The Right to Know and Access Personal Information

An individual shall have the right to request that a controller that collects personal information about the individual disclose to the individual:

(1) The specific pieces of personal information that the controller has collected about the individual; and

(2) The categories of sources from which the personal information has been collected.

SECTION 9. Right to Data Portability

(a) In response to a verifiable request pursuant to section 8 of this chapter, a controller shall disclose to the individual the information requested in the following manner:

(1) The controller shall provide to the individual the specific pieces of personal information that the controller has collected about the individual in a portable format that is easily understandable to the average individual and, to the extent technically feasible, in a readily usable format that allows the individual to transmit the information to another controller without hindrance. For the purposes of this subsection, “specific pieces of information” do not include any data generated to help ensure security and integrity.

(2) The controller shall also disclose the information specified in paragraph (2) of section 8 of this chapter, if so requested by the individual.

(3) The disclosure of the required information pursuant to paragraphs (1) and (2) of this subsection shall cover the 12 month period preceding the controller's receipt of the verifiable request; provided, however, that an individual may request that the controller disclose the required information beyond the 12 month period and the controller shall be required to provide such information unless doing so proves impossible or would constitute an undue burden for the controller. An individual's ability to request information beyond the 12 month period shall be clearly disclosed in a controller's privacy notice pursuant to clause (iii) of paragraph (1) of subsection (a) of section 7 of this chapter.

(b) Nothing in this section shall require a controller to provide the information requested in a manner that would disclose the controller's trade secrets.

SECTION 10. Right to Delete Personal Information

(a) An individual shall have the right to request that a controller delete any personal information provided by or obtained about the individual.

(b) A controller that receives a verifiable request to delete the individual's personal information shall, pursuant to section 17 of this chapter, delete the individual's personal information from its records, notify any processors to delete the individual's personal information from their records, and notify all third parties to whom the controller has sold the personal information to delete the individual's personal information unless doing so proves impossible or would constitute an undue burden for the controller.

(c) The controller may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of an individual who has submitted a deletion

request from being sold, for compliance with laws, or for other purposes solely to the extent permissible under this chapter.

(d) A controller, or a processor acting pursuant to its contract with the controller, shall not be required to comply with an individual's request to delete the individual's personal information if it is reasonably necessary for the controller or processor to maintain the individual's personal information in order to:

(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the individual or reasonably anticipated by the individual within the context of a controller's ongoing relationship with the individual, or otherwise perform a contract between the controller and the individual;

(2) Enable solely internal uses that are reasonably aligned with the expectations of the individual based on the individual's relationship with the controller and compatible with the context in which the individual provided the information; or

(3) Comply with a legal obligation.

(e) The controller or processor shall retain personal information pursuant to subsection (d) solely for the applicable purposes under that subsection.

SECTION 11. Right to Correct Personal Information

(a) An individual shall have the right to request that a controller correct inaccurate personal information concerning the individual, taking into account the nature of the personal information and the purposes of the processing of the personal information.

(b) A controller that receives a verifiable request to correct inaccurate personal information shall correct the inaccurate personal information as directed by the individual, pursuant to section 17 of this chapter.

SECTION 12. Right to Opt Out of the Sale of Personal Information

(a) An individual shall have the right to opt out of the processing of the individual's personal information for the purposes of the sale of such personal information. This shall also be known as the right to opt out of the sale of personal information.

(b) A controller shall comply with a request to exercise the right to opt out of the sale of personal information as soon as reasonably possible, but not later than 30 days after receipt of the request. A controller that has received direction from an individual not to sell the individual's personal information shall be prohibited from selling the individual's personal information unless the individual subsequently provides consent for the sale of the individual's personal information pursuant to subsection (c).

(c) After complying with an individual's request to exercise the right to opt out of the sale of their personal information, a controller shall wait for not less than 12 months before requesting the individual's consent to sell the individual's personal information.

(d) A data broker shall not sell an individual's personal information unless the individual has received explicit notice and is provided an opportunity to exercise the right to opt out of the sale of their personal information.

(e) If a controller communicates to any entity authorized by the controller to collect personal information that an individual has requested to exercise the right to opt out of the sale of

their personal information, that entity shall thereafter only use that individual's personal information for purposes specified by the controller, or as otherwise permitted by this chapter, and shall be prohibited from:

(1) Selling the personal information; and

(2) Retaining, using, or disclosing that individual's personal information: (i) for any purpose other than for the specific purpose of performing the services offered to the controller; (ii) outside of the direct relationship between the entity and the controller; or (iii) for a commercial purpose other than providing the services to the controller.

(f) A controller that communicates an individual's opt-out request to an entity pursuant to subsection (e) shall not be liable under this chapter if the entity receiving the opt-out request violates the restrictions set forth in this chapter; provided, however, that at the time of communicating the opt-out request, the controller does not know or should not reasonably know that the entity intends to commit such a violation.

SECTION 13. Right to Limit Use and Disclosure of Sensitive Information

(a) An individual shall have the right to direct a controller that collects sensitive information about the individual to limit its use of the individual's sensitive information to that use which is necessary to perform the services or provide the goods reasonably expected by an average individual who requests those goods or services or to perform the following services:

(1) Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of an individual's current interaction with the controller, provided that the individual's sensitive information is not disclosed to another third party and is not used to build a

profile about the individual or otherwise alter the individual's experience outside the current interaction with the controller;

(2) The performance of services on behalf of the controller, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the controller;

(3) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the controller, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the controller; or

(4) Helping to ensure security and integrity, to the extent the use of the individual's personal information is reasonably necessary and proportionate for those purposes.

(b) A controller shall comply with a request to exercise the right in subsection (a) as soon as reasonably possible, but not later than 30 days after receipt of the request. A controller that has received direction from an individual not to use or disclose the individual's sensitive information, except as authorized under this section, shall be prohibited from using or disclosing the sensitive information for any other purpose, unless the individual subsequently provides consent for the use or disclosure of the individual's sensitive information for additional purposes pursuant to subsection (c).

(c) For an individual who exercises the right in subsection (a), a controller shall wait for not less than 12 months before requesting the individual's consent to use and disclose the individual's sensitive information for additional purposes.

SECTION 14. Non-Discrimination Against Individuals' Good Faith Exercise of Privacy Rights

(a) A controller shall not discriminate against an individual for exercising, in good faith, any of the rights set forth in this chapter, including, but not limited to, by:

(1) Denying goods or services to the individual;

(2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;

(3) Providing a different level of quality of goods or services to the individual;

(4) Suggesting that the individual will receive a different price or rate for goods or services or a different level of quality or goods or services; or

(5) Retaliating against a job applicant to, an employee of, or an agent or independent contractor of the controller for exercising their rights under this chapter.

(b) This section shall not prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to an individual, including offering goods or services for no fee, if the offering is in connection with an individual's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

SECTION 15. Exercising Privacy Rights

(a) An individual may exercise the rights set forth in sections 8 through 13 of this chapter by submitting a request, at any time, to a controller specifying which rights the individual wishes to exercise.

(b) With respect to the processing of personal information of a child, the parent or legal guardian of the child may exercise the rights of this chapter on the child's behalf.

(c) With respect to the processing of personal information concerning an individual subject to guardianship, conservatorship, or other protective arrangement under article V or article 5A of chapter 190B of the General Laws, the guardian or the conservator of the individual may exercise the rights of this chapter on the individual's behalf.

(d) An individual may also designate an authorized agent to exercise, on behalf of that individual, the rights set forth in sections 12 and 13 of this chapter; provided, however, that:

(1) Unless the individual has provided the authorized agent with power of attorney pursuant to sections 5-501 through sections 5-507 of article V of chapter 190B of the General Laws, a controller receiving a request from an authorized agent to exercise these rights may require the authorized agent to provide proof that the individual gave the agent permission to submit the request; provided, further, that if the controller has a reasonable basis to believe that the proof submitted by the agent is insufficient or invalid, the controller may also require the individual to do either of the following: (i) verify the individual's own identity directly with the controller; or (ii) directly confirm with the controller that the individual provided the authorized agent with permission to submit the request; and

(2) An authorized agent shall not use an individual's personal information, or any information collected from or about the individual, for any purposes other than to fulfill the individual's requests, for verification, or for fraud prevention and shall implement and maintain reasonable security procedures and practices to protect the individual's personal information.

SECTION 16. Disclosure of Methods for Exercising Privacy Rights

(a) A controller shall make available, and shall describe in a privacy notice pursuant to section 7 of this chapter, not less than 2 designated methods for submitting a request to exercise the rights set forth in sections 8 through 13 of this chapter. If a controller maintains an Internet website, the controller shall make its Internet website available as one such designated method for submitting a request to exercise the rights set forth in said sections 8 through 13.

(b) A controller that sells individuals' personal information shall also provide a clear and conspicuous link on the controller's Internet homepages to an Internet web page that enables an individual, or an individual's authorized agent, to exercise their right to opt out of the sale of the individual's personal information.

(c) A controller that uses or discloses individuals' sensitive information for purposes other than those specified by section 13 of this chapter shall also provide a clear and conspicuous link on the controller's Internet homepages that enables an individual, or an individual's authorized agent, to limit the use or disclosure of the individual's sensitive information to those purposes authorized under said section 13.

(d) A controller that is subject to both subsections (b) and (c), in lieu of complying with both of those subsections, may utilize a single, clearly labeled link on the controller's Internet homepages, if that link easily allows an individual, or an individual's authorized agent, to exercise their right to opt out of the sale of the individual's personal information and to limit the use or disclosure of the individual's sensitive information.

(e) A controller shall:

(1) Ensure that all persons responsible for handling individuals' inquiries about the controller's privacy practices or the controller's compliance with this chapter are informed of: (i)

all requirements set forth under this chapter; and (ii) how to direct individuals to exercise their rights under sections 8 through 13 of this chapter;

(2) Include a separate link to the applicable web pages required under subsections (b), (c), or (d) of this section in any privacy notice that the controller is required to provide to individuals pursuant to section 7 of this chapter;

(3) Use any personal information collected from the individual in connection with the submission of the individual's request to exercise any of the rights set forth in sections 8 through 13 of this chapter solely for the purposes of complying with the request;

(4) Use any personal information collected in connection with the controller's verification of the individual's request solely for the purposes of verification and shall not further disclose the personal information, retain it longer than necessary for purposes of verification, or use it for unrelated purposes; and

(5) Not require an individual to provide additional information beyond what is necessary to direct the controller to not sell the individual's personal information pursuant to section 12 of this chapter, or to limit use or disclosure of the individual's sensitive information pursuant to section 13 of this chapter.

SECTION 17. Responding to an Individual's Request

(a) Except as otherwise provided in this chapter, a controller shall comply with a request to exercise the rights set forth in sections 8 through 11 of this chapter.

(b) A controller shall inform the individual of any action taken on a request to exercise any of the rights set forth in sections 8 through 11 of this chapter without undue delay and in any

event within 45 days of receipt of the request; provided, however, that the period may be extended once by 45 additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller shall notify the individual of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(c) A controller shall not be obligated to comply with a request to exercise the rights set forth in sections 8 through 11 of this chapter if the request is not a verifiable request. In such a case, the controller shall notify the individual that it is unable to act on the request until it receives additional information reasonably necessary to verify that the request is being made by the individual or by another person who is entitled to exercise such rights on behalf of the individual pursuant to subsections (b) and (c) of section 15 of this chapter.

(d) A verifiable request to exercise the rights set forth in sections 8 through 11 of this chapter shall not extend to personal information about the individual that belongs to, or the controller maintains on behalf of, another natural person. A controller may rely on representations made in a verifiable request as to rights with respect to personal information and shall not be required to seek out other persons that may have or claim to have rights to personal information or to take any action under this chapter in the event of a dispute between or among persons claiming rights to personal information in the controller's possession.

(e) A request to exercise any of the rights in sections 12 or 13 of this chapter shall not need to be a verifiable request. If a controller, however, has a good-faith, reasonable, and documented belief that the request is fraudulent, the controller may deny the request. The controller shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

(f) When a controller, pursuant to subsection (b) of section 23 of this chapter, is incapable of complying with an individual's verifiable request, the controller shall, if possible, notify the individual that it is not in a position to identify the individual. The individual, or a person entitled to exercise the rights of this chapter on behalf of the individual pursuant to subsections (b) and (c) of section 15 of this chapter, may provide additional information to the controller enabling the individual's identification for the purposes of exercising their rights set forth in sections 8 through 11 of this chapter.

(g) If a controller declines to take action regarding an individual's request, the controller shall notify the individual of the justification for declining to take action and provide the individual with instructions on how to submit a complaint pursuant to subsection (j) of this section. Such notification shall occur without undue delay, but not later than 45 days after the initial receipt of the request or not later than 45 days after notifying the individual of the applicability of an extension pursuant to subsection (b) of this section.

(h) A controller shall not be obligated to provide the information required by section 9 of this chapter to the same individual more than twice in a 12 month period. Information provided in response to a request shall be provided by the controller to the individual free of charge.

(i) If requests from an individual, or from a person entitled to exercise the rights of this chapter on behalf of such individual pursuant to subsections (b) and (c) of section 15 of this chapter, are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may: (1) charge a reasonable fee to cover the administrative costs of complying with the request; or (2) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive nature of the request.

(j) When informing an individual of any action taken or not taken in response to a request, the controller shall provide the individual with a link to the Attorney General's online mechanism through which the individual may contact the Attorney General to submit a complaint. The controller shall maintain records of all rejected requests for not less than 24 months and shall compile and provide a copy of such records to the Attorney General upon the Attorney General's request.

SECTION 18. No Waiver

Any provision of a contract or agreement of any kind that purports to waive or limit in any way individual rights under this chapter shall be deemed contrary to public policy and shall be void and unenforceable.

SECTION 19. Relationship Between Controllers and Processors

(a) A processor shall not be required to comply with a request pursuant to sections 8 through 13 of this chapter that the processor receives directly from an individual or from a person entitled to exercise such rights on behalf of the individual, to the extent that the processor has processed the individual's personal information on behalf of the controller. A processor shall adhere to the instructions of the controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include, but not be limited to, the following:

(1) Taking into account the nature of the processing and the information available to the processor, the processor shall assist the controller by taking appropriate technical and organizational measures, if possible, to fulfill the controller's obligation to respond to individuals' requests to exercise their rights pursuant to sections 8 through 13 of this chapter, including by:

(i) Providing to the controller the individual's personal information, or correcting inaccurate personal information, in the processor's possession that the processor obtained as a result of providing services to the controller, or enabling the controller to do the same;

(ii) At the direction of the controller in response to a verifiable request pursuant to section 10 of this chapter, deleting or enabling the controller to delete personal information about the individual processed by the processor on behalf of the controller; provided, however, that the processor shall notify any processors or third parties who may have accessed personal information from or through the processor to delete the individual's personal information, unless the information was accessed at the direction of the controller or unless doing so proves impossible or would constitute an undue burden; or

(iii) Not using sensitive information, after it has received instructions from the controller and to the extent it has actual knowledge that the personal information is sensitive information, for any purpose other than those authorized by section 13 of this chapter; provided, however, that the processor shall only be required to limit its use of sensitive information received pursuant to a written contract with the controller in response to instructions from the controller and only with respect to its relationship with that controller;

(2) Taking into account the nature of the processing and the information available to the processor, the processor shall assist the controller in meeting the controller's obligations in relation to the security of processing the personal information and in relation to the notification of a breach of security of the system of the processor, pursuant to chapter 93H of the General Laws; and

(3) The processor shall provide information to the controller necessary to enable the controller to conduct and document any risk assessments required by section 21 of this chapter.

(b) Notwithstanding the instructions of the controller, a processor shall ensure that each person processing personal information is subject to a duty of confidentiality with respect to the information.

(c) If a processor engages another entity to assist the processor in processing personal information on behalf of the controller, the processor shall provide the controller with an opportunity to object and the engagement shall be pursuant to a written contract, in accordance with subsection (e), that requires the entity to meet the obligations of the processor with respect to the personal information.

(d) The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement such measures.

(e) A contract between a controller and a processor shall govern the processor's procedures with respect to processing individuals' personal information that the processor receives from or on behalf of the controller. The contract shall be binding on both parties and clearly set forth the processing instructions to which the processor is bound, including:

(1) The nature and purpose of the processing;

(2) The type of personal information subject to the processing;

(3) The duration of the processing;

(4) The rights and obligations of both parties;

(5) The requirements imposed by subsections (b) and (c); and

(6) The following requirements:

(i) At the controller's direction, the processor shall delete or return all personal information to the controller as requested at the end of the provision of services, unless retention of the personal information is required by law;

(ii) Upon the reasonable request of the controller, the processor shall make available to the controller all information in its possession necessary to demonstrate compliance with the obligations under this chapter;

(iii) The processor shall: (A) allow for, and cooperate with, reasonable audits and inspections by the controller or the controller's designated auditor; or (B) arrange for, with the controller's consent, a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and audit procedure for such audits, provided that the processor shall disclose a report of the audit to the controller upon request; and

(iv) The processor shall be prohibited from: (A) selling the personal information; (B) retaining, using, or disclosing personal information other than for the purposes specified in the contract or as otherwise permitted by this chapter; (C) retaining, using, or disclosing personal information outside of the direct relationship between the processor and the controller; or (D) combining, for the purpose of targeted advertising, the personal information with the personal information that the processor receives from, or on behalf of, another entity or entities or that it collects from its own interaction with the individual.

(f) In no event may any contract relieve a controller or a processor from the liabilities imposed on it by this chapter.

(g) Determining whether an entity is acting as a controller or processor with respect to a specific processing of information is a fact-based determination that depends upon the context in which personal information is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal information remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal information, it is a controller with respect to the processing. An entity that is not limited in its processing of personal information pursuant to a controller's instruction, or that fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing.

SECTION 20. Data Broker Registration

(a) Not later than January 31 following each year in which a controller meets the definition of a data broker under this chapter, the controller shall register with the Attorney General pursuant to the requirements of this section.

(b) When registering with the Attorney General, a data broker shall:

(1) Pay a registration fee of 200 dollars; and

(2) Provide the following information:

(i) The name of the data broker and its primary physical, email, and Internet website addresses;

(ii) Any privacy notice that a data broker discloses to individuals pursuant to section 7 of this chapter;

(iii) How and where individuals may request to exercise the rights under sections 12 and 13 of this chapter;

(iv) Whether the data broker implements a purchaser credentialing process;

(v) Whether the data broker sells the personal information of individuals with whom the data broker does not have a direct relationship;

(vi) Whether the data broker sells the sensitive information of at least 10,000 individuals;

(vii) Whether the data broker processes the personal information of minors or children; and

(viii) Any additional information or explanation the data broker may wish to provide.

SECTION 21. Risk Assessments

(a) If a type of processing, taking into account the nature, scope, context and purposes of the processing and whether the processing involves new technologies, is likely to result in a high risk of harm to the individual, the controller shall, prior to the processing, carry out a risk assessment of the impact of the envisioned processing operations on the protection of personal information. A single assessment may address a set of similar processing operations that present similar high risks.

(b) In particular, a controller shall conduct a risk assessment in the case of:

(1) The processing of sensitive information;

(2) The sale of personal information; or

(3) A systematic and extensive evaluation of personal aspects relating to individuals that is based on automated processing, on which decisions are based that present a reasonably foreseeable risk of: (i) unfair or deceptive treatment of, or unlawful disparate impact on, certain individuals; (ii) financial, physical, or reputational harm to individuals; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of individuals, where such intrusion would be offensive to a reasonable person; or (iv) other substantial cognizable harms to individuals.

(c) The assessment shall contain at a minimum:

(1) A systematic description of the envisioned processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller or third party;

(2) An assessment of the necessity of the processing operations in relation to the purposes, taking into account whether the controller or third party can achieve their legitimate interests in another less intrusive way;

(3) An assessment of the proportionality of the processing operations in relation to the purposes, taking into account the amount and nature of the personal information to be processed;

(4) An assessment of the risks to individuals;

(5) The measures envisioned to address the risks, including safeguards such as de-identification, security measures and mechanisms to ensure the protection of personal

information and to demonstrate compliance with this chapter taking into account the individuals' reasonable expectations of privacy or other legal rights; and

(6) A description of: (i) the context of the processing; (ii) the relationship between the controller and the individual whose personal information would be processed; and (iii) whether the controller is processing an individual's personal information in ways in which the individual would reasonably expect.

(d) Subsections (a) through (c) shall not apply to processing pursuant to paragraph (3) of section 6 of this chapter that has a legal basis in any federal or state law to which the controller is subject; provided, however, that the law regulates the specific processing operation or set of operations in question and the controller has already carried out a risk assessment that has reasonably comparable scope and effect for the purpose of compliance with that law.

(e) Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the risk assessment at least when there is a change of the risk represented by processing operations.

(f) A controller shall implement procedures to comply with this section that are reasonable and appropriate taking into consideration:

(1) The size, scope, and type of the controller;

(2) The amount of resources available to the controller;

(3) The amount and nature of personal information processed by the controller, including, but not limited to, whether the personal information is sensitive information; and

(4) The need for the security and confidentiality of the personal information processed by the controller.

(g) The Attorney General may require, pursuant to a civil investigative demand, that a controller disclose any risk assessment that is relevant to an investigation conducted by the Attorney General. The controller shall accordingly make the risk assessment available to the Attorney General, and the Attorney General may evaluate the risk assessment for compliance with the responsibilities in this chapter. Risk assessments shall be confidential and exempt from public inspection and copying under chapter 66 of the General Laws. The disclosure of a risk assessment pursuant to a civil investigative demand 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.

(h) Risk assessments shall apply to processing activities created or generated after this chapter is enacted and shall not be retroactive.

SECTION 22. Processing That Unlawfully Discriminates

(a) A controller that processes personal information in a manner that violates chapter 151B of the General Laws or any other state or federal law prohibiting unlawful discrimination against individuals shall also be in violation of this chapter.

(b) Nothing in this section shall be construed to limit controllers from processing personal information for legitimate testing to prevent unlawful discrimination or otherwise determine the extent or effectiveness of the controller’s compliance with this section.

SECTION 23. De-identified Information

(a) A controller that possesses de-identified information shall:

(1) Take reasonable technical and organizational measures to ensure that the information cannot be associated with an identified or identifiable individual or household;

(2) Not attempt to re-identify the information, provided that the controller may attempt to re-identify the information solely for the purpose of determining whether its de-identification procedures satisfy the requirements of this subsection; and

(3) Contractually require any recipients of the information to comply with all the requirements of this subsection.

(b) This chapter shall not be construed to require a controller or processor to do any of the following solely for the purpose of complying with this chapter:

(1) Maintain information in an identifiable, linkable, or associable form, or collect, obtain, retain, or access any information or technology, in order to be capable of linking or associating a verifiable request with personal information; or

(2) Reidentify or otherwise link de-identified information, provided that the controller provides applicable notice to the individual pursuant to subsection (f) of section 17 of this chapter.

SECTION 24. Limitations.

(a) The obligations imposed on controllers or processors under this chapter shall not restrict a controller’s or a processor’s ability to:

(1) Comply with federal, state, or local laws, rules or regulations;

(2) Comply with a civil, criminal, or regulatory inquiry, subpoena, or summons by federal, state, local, 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 local laws, rules, or regulations;

(4) Investigate, establish, exercise, prepare for, or defend legal claims;

(5) Take immediate steps to protect the security or protection of an individual or another natural person, if that individual or other natural person is at risk or danger of death or serious physical injury; or

(6) Assist another controller, processor, or third party with any of the obligations under this subsection.

(b) The obligations imposed on controllers or processors under sections 8 through 13 of this chapter shall not restrict a controller or processor's ability to retain or process information for the following purposes, provided that the use of the individual's personal information is reasonably necessary and proportionate for the purposes:

(1) Helping to ensure security and integrity;

(2) Debugging to identify and repair errors that impair existing intended functionality;

(3) Fulfilling the terms of a written warranty or product recall conducted in accordance with federal law;

(4) Engaging in public or peer-reviewed scientific, historical, or statistical research in the public interest that conforms or adheres to all other applicable ethics and privacy laws; provided, however, that:

(i) Such research is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines: (A) if the research 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 reidentification; or

(ii) A controller's deletion of the personal information pursuant to a request under section 10 of this chapter is likely to render impossible or seriously impair the ability to complete such research.

(d) Obligations imposed on controllers or processors under this chapter shall not:

(1) Apply to the processing of personal information by a natural person in the course of a purely personal or household activity;

(2) Apply where compliance by the controller or processor would violate an evidentiary privilege under the laws of the Commonwealth or be construed to prevent a controller or processor from providing personal information concerning an individual to a person covered by an evidentiary privilege under the laws of the Commonwealth as part of a privileged communication;

(3) Adversely affect the right of an individual or any other person to exercise free speech, pursuant to the First Amendment to the United States Constitution, or to exercise another right provided for by law; or

(4) Apply to an entity's publication of entity-based member or employee contact information where such publication is intended to allow members of the public to contact such member or employee in the ordinary course of the entity's operations.

(e) Personal information that is processed by a controller pursuant to an exemption under subsections (a) through (d) of this section:

(1) Shall not be processed for any purpose other than those expressly listed in subsections (a) through (d), unless otherwise allowed by this chapter; and

(2) Notwithstanding anything in this section to the contrary, shall be processed in accordance with section 5 of this chapter and subject to reasonable administrative, technical, and physical measures to reduce reasonably foreseeable risks of harm to individuals.

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

(g) A controller or processor that discloses personal information to a processor or third party in compliance with the requirements of this chapter is not in violation of this chapter if the recipient processes such personal information in violation of this chapter; provided, however, that at the time of disclosing the personal information, the disclosing controller or processor did not know or should not reasonably have known that the recipient intended to commit a violation.

(h) A processor or third party receiving personal information from a controller or processor in compliance with the requirements of this chapter is not in violation of this chapter if the controller or processor from which it receives the personal information fails to comply with applicable obligations under this chapter; provided, however, that the processor or third party shall be liable for its own violations of this chapter.

(i) If an individual has already consented to a controller's use, disclosure, or sale of their personal information to produce a physical item, such as a school yearbook, sections 10 through 13 of this chapter shall not apply to the controller's use, disclosure, or sale of the particular pieces of the individual's personal information for the production of that physical item; provided, however, that:

(1) The controller has incurred significant expense in reliance on the individual's consent;

(2) Compliance with the individual's request to exercise any of the rights in sections 10 through 13 would not be commercially reasonable; and

(3) The controller complies with the individual's request as soon as it is commercially reasonable to do so.

SECTION 25. Powers of the Attorney General

(a) Whenever the Attorney General of the Commonwealth has reasonable cause to believe that an entity has engaged in, is engaging in, or is about to engage in a violation of this chapter, the Attorney General may issue a civil investigative demand. The provisions of section 6 of chapter 93A of the General Laws shall apply mutatis mutandis to civil investigative demands issued under this chapter.

(b) The Attorney General shall have the authority to enforce the provisions of this chapter. A violation of this chapter shall not serve as the basis for or be subject to a private right of action under this chapter. Nothing in this chapter shall be construed as creating a new private right of action or serving as the basis for a private right of action that would not otherwise have had a basis under any other law but for the enactment of this chapter. This chapter neither relieves any party from any duties or obligations imposed, nor alters any independent rights that individuals have, under chapter 93A of the General Laws, other state or federal laws, the Massachusetts Constitution, or the United States Constitution.

(c) Prior to initiating any civil action under this chapter, the Attorney General shall provide an entity written notice identifying the specific provisions of this chapter that the Attorney General alleges have been or are being violated.

(d) (1) The entity shall have a period of 30 days in which to cure a violation after being provided notice by the Attorney General. If within that time period the entity 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 shall be initiated against the entity.

(2) Paragraph (1) shall not apply when:

(i) The court has previously issued a temporary restraining order, preliminary injunction, or permanent injunction or assessed civil penalties against the entity for a violation of this chapter;

(ii) The Attorney General and the entity have previously reached a settlement relating to this chapter that includes an admission by the entity that it has violated this chapter, not including any express written statement provided pursuant to paragraph (1);

(iii) The Attorney General has clear and convincing evidence that the entity willfully and wantonly violated this chapter;

(iv) The violation is a data broker's failure to register pursuant to section 20 of this chapter; or

(v) The violation occurs more than twenty four months after the effective date of this section and the violating entity: (A) as of January 1 of the calendar year, had annual global gross revenues in excess of 1,000,000,000 dollars in the preceding calendar year; and (B) determines the purposes and means of processing of the personal information of not less than 100,000 individuals.

(3) In its notice pursuant to subsection (c), the Attorney General shall specify the length, if any, of the period in which the entity can cure the noticed violation.

(e) If an entity continues to violate this chapter following the cure period in subsection (d), breaches an express written statement provided to the Attorney General under that subsection, or is not eligible for a cure period pursuant to that subsection, the Attorney General may initiate a civil action against the entity in the name of the Commonwealth or as parens patriae on behalf of individuals. The Attorney General may seek a temporary restraining order, preliminary injunction, or permanent injunction to restrain any violations of this chapter and may seek civil penalties of up to 7,500 dollars for each violation under this chapter, not including violations of section 20 of this chapter.

(f) The superior court shall have jurisdiction of actions brought under this section. Such actions may be brought in any county where a defendant resides or has its principal place of business or in which the violation occurred in whole or in part, or, with the consent of a defendant, in the superior court for Suffolk County.

(g) In determining the overall amount of civil penalties to seek or assess against an entity, the Attorney General or the court shall include, but not be limited to, the following in its consideration:

(1) The size, scope, and type of the entity;

(2) The amount of resources available to the entity;

(3) The amount and nature of personal information processed by the entity;

(4) The number of violations;

(5) The number of violations affecting minors or children;

(6) The nature and severity of the violation;

(7) The risks caused by the violation;

(8) Whether the entity's violation was not an isolated instance but instead part of a pattern of violations and noncompliance with this chapter;

(9) Whether the entity is a data broker that did not register pursuant to section 20 of this chapter;

(10) Whether the violation was willful and not the result of error;

(11) The length of time over which the violation occurred;

(12) The precautions taken by the entity to prevent a violation;

(13) The good faith cooperation of the entity with any investigations conducted by the Attorney General pursuant to this section;

(14) Efforts undertaken by the entity to cure the violation; and

(15) The entity's past violations of information privacy rules, regulations, codes, ordinances, and laws in other jurisdictions.

(h) A data broker that fails to register as required by section 20 of this chapter may be subject to injunction and liable for civil penalties, fees, and costs in a civil action brought on behalf of the Commonwealth by the Attorney General as follows:

(1) A civil penalty of up to 500 dollars for each day, not to exceed a total of 100,000 dollars for each year, the data broker fails to register as required by this section; and

(2) Fees equal to the fees that were due during the period the data broker failed to register.

(i) Any entity that violates the terms of an injunction or other order issued under this section shall forfeit and pay a civil penalty of up to 10,000 dollars for each violation. For the purposes of this section, the court issuing such an injunction or order shall retain jurisdiction, and the cause shall be continued, and in such case the Attorney General acting in the name of the Commonwealth may petition for recovery of such civil penalty.

(j) The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in any action initiated under this chapter.

(k) If two or more entities are involved in the same processing that violates this chapter, the liability shall be allocated among the parties according to principles of comparative fault.

(l) Notwithstanding any general or special law to the contrary, the court may require that the amount of a civil penalty imposed pursuant to this section exceeds the economic benefit realized by an entity for noncompliance.

(m) If a series of steps or transactions were component parts of a single transaction intended to avoid the reach of this chapter, the Attorney General and the court shall disregard the intermediate steps or transactions and consider everything one transaction for purposes of effectuating the purposes of this chapter.

(n) Not later than 30 days after the end of each calendar year, the Attorney General shall publish a public, easily accessible report that provides, for that calendar year, the following information:

(1) Anonymized examples of alleged violations that have been cured by an entity pursuant to subsection (d); provided, however, that these examples shall protect the confidentiality of the entity;

(2) The number of written notices issued pursuant to subsection (c);

(3) The number of entities that received written notices issued pursuant to subsection (c); and

(4) The categories of violations of this chapter and the number of violations per category.

(o) The Attorney General shall receive and may investigate sworn complaints from an individual or other natural person that an entity has engaged in, is engaging in, or is about to engage in any violation of this chapter. The Attorney General shall notify the individual or other natural person who made the complaint of the action, if any, the Attorney General has taken or plans to take on the complaint, together with the reasons for that action or nonaction.

(p) The Attorney General shall maintain the following Internet web pages: (1) a web page that includes an online mechanism through which any individual or other natural person may contact the Attorney General to submit a sworn complaint; (2) a web page that enables data brokers to register pursuant to section 20 of this chapter; and (3) a web page that makes publicly accessible the information provided by data brokers pursuant to section 20 of this chapter.

(q) The Attorney General shall promote public awareness and understanding of the risks, rules, responsibilities, safeguards, and rights in relation to the processing of personal information, including the rights of individuals under the age of 16 with respect to their own information. The Attorney General shall provide guidance to individuals regarding what to do if they believe their rights under this chapter have been violated.

(r) The Attorney General shall create and make publicly accessible the following templates: (1) a template privacy policy that meets the requirements of section 7 of this chapter; (2) a template contract between a controller and a processor that meets the requirements of section 19 of this chapter; and (3) a template risk assessment that meets the requirements of section 21 of this chapter.

(s) The Attorney General shall have the power to determine, pursuant to section 27 of this chapter, whether the provisions of a personal information privacy law in another jurisdiction are equally or more protective of personal information than the provisions in this chapter.

(t) The Attorney General shall establish a mechanism pursuant to which an entity that processes the personal information of one or more individuals but does not meet the applicability criteria set forth in subsection (b) of section 3 of this chapter may voluntarily certify that it is in compliance with, and agrees to be bound by, this chapter. The Attorney General shall make a list of those entities available to the public.

(u) The Attorney General shall adopt regulations for the purposes of carrying out this chapter, including, but not limited to, the following areas:

(1) Supplementing any of the definitions used in this chapter or adding in new definitions for terms that are used but not otherwise defined in this chapter, in order to address changes in technology, data collection, obstacles to implementation, and privacy concerns; and

(2) Ensuring that the notices and information that controllers are required to provide pursuant to section 7 of this chapter are provided in a manner that may be easily understood by the average individual, are accessible to individuals with disabilities, and are available in the language primarily used to interact with the individual.

(v) The Attorney General shall conduct research and monitor relevant developments relating to the protection of personal information, the development of information and communication technologies and commercial practices, and the enactment and implementation of privacy laws in other states, territories, and countries or by the federal government. Specific

topics for research by the Attorney General shall include, but are not limited to, the following areas:

(1) The available best methods for an individual to exercise the rights set forth in sections 8 through 13 of this chapter, including: (i) the development of technology, such as a browser setting, browser extension, or global device setting, indicating an individual's affirmative, freely given, and unambiguous choice to opt out of the sale of the individual's personal information or to limit the use or disclosure of the individual's sensitive information; (ii) the development of technology that enables an individual to opt out of the sale of the individual's personal information by all data brokers that have registered pursuant to section 20 of this chapter; and (iii) ways for entities to conspicuously and clearly disclose how to exercise the rights set forth in sections 8 through 13;

(2) Access and opt-out rights with respect to controllers' use of automated decision-making technology;

(3) Eye-tracking technology and targeted advertising based on information collected through eye-tracking technology;

(4) Financial incentive programs offered by controllers for the processing of personal information;

(5) The targeting of advertising based on a profile of an individual created by an individual's activity over time with regard to an entity's own businesses, distinctly-branded websites, applications, or services;

(6) The data broker industry, including data brokers that have registered pursuant to section 20 of this chapter;

(7) The effectiveness of allowing an individual to designate an authorized agent to exercise a right on their behalf pursuant to subsection (d) of section 15 of this chapter; and

(8) Whether to change or eliminate the cure period established in subsection (d) of section 25 of this chapter.

(w) At least once per calendar year, the Attorney General shall provide a full written report to the Legislature's Joint Committee on Advanced Information Technology, the Internet and Cybersecurity. The report shall summarize the Attorney General's research and any recommendations with respect to privacy-related legislation. The first such report provided by the Attorney General shall be submitted within 12 months of the effective date of this subsection and shall include a summary of the Attorney General's research and recommendations pursuant to paragraphs (1) through (5) of subsection (v).

(x) The monetary amounts referred to in this chapter shall be indexed for inflation by the Attorney General, who, not later than December 31 of each even numbered year, shall calculate and publish such indexed amounts, using the federal consumer price index for the Boston statistical area and rounding to the nearest dollar.

SECTION 26. Massachusetts Privacy Fund.

(a) There shall be established upon the books of the Commonwealth a separate special fund to be known as the Massachusetts Privacy Fund.

(b) All civil penalties, expenses, attorney fees, and registration fees collected pursuant to sections 20 and 25 of this chapter shall be paid into the state treasury and credited to the Massachusetts Privacy Fund. Interest earned on moneys in the Fund shall remain in the Fund and be credited to it. Any moneys remaining in the Fund, including interest thereon, at the end of each fiscal year shall not revert to the general fund but shall remain in the Fund.

(c) The Attorney General shall have discretion to allocate the proceeds of any settlement of a civil action pursuant to this chapter to: (1) the Massachusetts Privacy Fund; (2) the general fund; or (3) where possible, directly to individuals impacted by the violation of the chapter.

(d) Moneys in the Massachusetts Privacy Fund shall be used to support the work of the Attorney General pursuant to section 25 of this chapter. Moneys in the Massachusetts Privacy Fund shall be subject to appropriation and shall not be used to supplant general fund appropriations to the Attorney General.

SECTION 27. Reciprocity and Interoperability

(a) A controller or processor shall be in compliance with provisions of this chapter if: (1) it complies with comparable provisions of a personal information privacy law in another jurisdiction; (2) the controller or processor applies the provisions of that law to its processing activities concerning individuals; and (3) the Attorney General determines that the provisions of that law in the other jurisdiction are equally or more protective of personal information than the provisions of this chapter.

(b) The Attorney General may charge a fee to a controller or processor that asserts compliance with a comparable law under subsection (a); provided, however, that the fee shall

reflect costs reasonably expected to be incurred by the Attorney General to determine whether the provisions of said law are equally or more protective than the provisions of this chapter.

SECTION 28. Delayed Implementation for Nonprofits and Institutions of Higher Education

This chapter shall not apply to institutions of higher education or nonprofit organizations until 24 months after the effective date of this section.

SECTION 29. Severability

(a) The provisions of this chapter are severable. If any provision of this chapter, or the application of any provision of this chapter, is held invalid, the remaining provisions, or applications of provisions, shall remain in full force and not be affected.

(b) If a court were to find in a final, unreviewable judgment that the exclusion of one or more entities or activities from the applicability of this chapter renders the chapter unconstitutional, those exceptions shall be rendered null and invalid and the exemption shall not continue.

SECTION 2. Chapter 93H of the General Laws is hereby amended by inserting after section 6 of said chapter the following section:

SECTION 7. Private Right of Action and Safe Harbor

(a) For the purposes of this section, the term “personal information” shall have the same meaning as defined in section 1 of this chapter, except that for the purposes of subsections (c) and (d) of this section, the term “personal information” shall have the same meaning as in section 2 of chapter 93M of the General Laws.

(b) For the purposes of this section, the following terms shall have the same meanings as such terms are defined in section 2 of chapter 93M of the General Laws: “controller”; “data broker,” “individual”; “process”; and “sell.”

(c) This section shall apply to a controller that:

(1) Conducts business in the Commonwealth or is not physically established in the Commonwealth but processes personal information where such processing activities are related to: (i) the offering of goods or services that are targeted to individuals; or (ii) the monitoring of behavior of individuals where such behavior takes place in the Commonwealth; and

(2) Meets 1 of the following additional thresholds:

(i) The controller, as of January 1 of the calendar year, had annual global gross revenues in excess of 25,000,000 dollars in the preceding calendar year;

(ii) The controller determines the purposes and means of processing of the personal information of not less than 100,000 individuals; or

(iii) The controller is a data broker.

This section shall also apply to an entity that is an affiliate of and shares common branding with such a controller, with respect to the personal information processed by the affiliate on behalf of the controller.

(d) This section shall not apply to controllers and information that are fully exempt from the provisions of chapter 93M of the General Laws pursuant to section 3 of that chapter; provided, however, that this section shall apply to an activity involving the processing of any personal information bearing on an individual’s credit worthiness, credit standing, credit

capacity, character, general reputation, personal characteristics, or mode of living by: (A) a consumer reporting agency, as defined in 15 U.S.C. 1681a(f); (B) a furnisher of information, as set forth in 15 U.S.C. 1681s-2, that provides information for use in a consumer report, as defined in 15 U.S.C. 1681a(d); and (C) a user of a consumer report, as set forth in 15 U.S.C. 1681b.

(e) Any individual whose personal information is subject to a breach of security, as defined in section 1 of this chapter, as a result of a controller's failure to implement and maintain reasonable cybersecurity controls may institute a civil action for any of the following:

(1) Damages from the controller in an amount up to 500 dollars per individual per incident or actual damages, whichever is greater;

(2) Injunctive or declaratory relief;

(3) Any other relief the court deems proper.

(f) In assessing the amount of statutory damages against the controller, the court shall include, but not be limited to, the following in its consideration:

(1) The size, scope, and type of the entity;

(2) The amount of resources available to the entity;

(3) The amount and nature of personal information processed by the entity;

(4) The number of violations;

(5) The number of violations affecting minors or children;

(6) The nature and severity of the violation;

(7) The risks caused by the violation;

(8) Whether the entity's violation was not an isolated instance but instead part of a pattern of violations and noncompliance with this chapter;

(9) Whether the entity is a data broker that did not register pursuant to section 20 of chapter 93M of the General Laws;

(10) Whether the violation was willful and not the result of error;

(11) The length of time over which the violation occurred;

(12) The precautions taken by the entity to prevent a violation;

(13) The good faith cooperation of the entity;

(14) Efforts undertaken by the entity to cure the violation; and

(15) The entity's past violations of rules, regulations, codes, ordinances, and laws in other jurisdictions regarding breaches of security.

(g) In any cause of action founded in tort that is brought pursuant to this section and that alleges that the controller's failure to implement reasonable cybersecurity controls resulted in a breach of security concerning personal information, the court shall not assess punitive damages against a controller if such controller:

(1) Created, maintained and complied with a written cybersecurity program that contains administrative, technical and physical safeguards for the protection of personal information and that conforms to an industry recognized cybersecurity framework, as described in subsection (i); and

(2) Designed its cybersecurity program in accordance with the provisions of subsections (k) and (l).

(h) Subsection (g) shall not apply if the controller's failure to implement reasonable cybersecurity controls was the result of gross negligence or willful or wanton conduct.

(i) A controller's cybersecurity program, as described in subsection (g), shall conform to an industry recognized cybersecurity framework if:

(1) The cybersecurity program conforms to the current version of or any combination of the current versions of:

(i) The "Framework for Improving Critical Infrastructure Cybersecurity" published by the National Institute of Standards and Technology;

(ii) The National Institute of Standards and Technology's special publication 800-171;

(iii) The National Institute of Standards and Technology's special publications 800-53 and 800-53a;

(iv) The Federal Risk and Authorization Management Program's "FedRAMP Security Assessment Framework";

(v) The Center for Internet Security's "Center for Internet Security Critical Security Controls for Effective Cyber Defense"; or

(vi) The "ISO/IEC 27000-series" information security standards published by the International Organization for Standardization and the International Electrotechnical Commission; or

(2) The cybersecurity program complies with the current version of the "Payment Card Industry Data Security Standard" and the current version of another applicable industry recognized cybersecurity framework described in paragraph (1) of this subsection.

(j) When a revision to a document listed in paragraph (1) or (2) of subsection (i) is published, a controller whose cybersecurity program conforms to a prior version of that document shall be said to conform to the current version of that document if the controller conforms to such revision not later than six months after the publication date of the revision.

(k) For the purposes of complying with this section, a controller's cybersecurity program shall be implemented in accordance with the regulations adopted pursuant to chapter 93H of the General Laws.

(l) The scale and scope of a controller's cybersecurity program shall be based on:

(1) The size, scope and type of controller obligated to safeguard the personal information under such program;

(2) The amount of resources available to the controller;

(3) The amount and nature of personal information processed by the controller; and

(4) The reasonably foreseeable risks to the security and confidentiality of the personal information processed by the controller.

(m) The cause of action established by this section shall apply only to violations as defined in this section. This chapter neither relieves any party from any duties or obligations imposed, nor alters any independent rights that individuals have under chapter 93A of the

General Laws, other state or federal laws, the Massachusetts Constitution or the United States Constitution.

(n) Nothing in this section shall limit the authority of the Attorney General to initiate actions as otherwise allowed in this section or pursuant to any other general law.

SECTION 4. Chapter 93M of the General Laws shall take effect 18 months after the passage of this act, except that section 2 and subsections (p) through (w) of section 25 of said chapter shall take effect upon the passage of this act.

SECTION 5. Section 2 of this act shall take effect 18 months after the passage of this act.