SENATE DOCKET, NO. 2355   FILED ON: 1/17/2025

SENATE . . . . No.

The Commonwealth of Massachusetts

PRESENTED BY:

Barry R. Finegold

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act advancing the economic development of the commonwealth through comprehensive data privacy.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
Barry R. Finegold	*Second Essex and Middlesex*

SENATE DOCKET, NO. 2355   FILED ON: 1/17/2025

SENATE . . . . No.

[Pin Slip]

[SIMILAR MATTER FILED IN PREVIOUS SESSION
SEE SENATE, NO. *227* OF 2023-2024.]

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Fourth General Court
(2025-2026)

An Act advancing the economic development of the commonwealth through comprehensive data privacy.

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:

"Affiliate", an entity that controls, is controlled by or is under common control or shares common branding with another entity; provided, however, that for the purposes of this definition, "control" or "controlled" shall mean:

(i) ownership of more than 50 per cent of the outstanding shares of any class of voting security of the entity;

(ii) control in any manner over the election of a majority of the entity's directors or of persons exercising similar functions; or

(iii) the power to otherwise exercise a controlling influence over the management of the entity.

"Biometric information", a retina or iris scan, fingerprint, voiceprint, map or scan of hand or face geometry, vein pattern, gait pattern or other personal information generated from the specific technical processing of an individual's unique biological or physiological patterns or characteristics used to identify a specific individual; provided, however, that "biometric information" shall not include:

(1) a digital or physical photograph;

(2) an audio or video recording; or

(3) data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

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

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

"Collect", buy, rent, gather, obtain, receive or otherwise access any personal information pertaining to an individual by any means including, but not limited to, obtaining information from an individual, either actively or passively, or by observing an individual's behavior.

"Common branding", a shared name, service mark, trademark or other indicator that an individual would reasonably understand to indicate that 2 or more entities are commonly owned.

"Consent", a clear affirmative act signifying an individual's freely given, specific, informed and unambiguous agreement to allow the processing of specific categories of personal information relating to the individual for a narrowly defined particular purpose; provided, however, that "consent" may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action; and provided further, that the following shall not constitute "consent":

(i) acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information;

(ii) hovering over, muting, pausing or closing a given piece of content; or

(iii) agreement obtained through dark patterns or a false, fictitious, fraudulent or materially misleading statement or representation.

"Controller", 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", a user interface that is designed, modified or manipulated with the purpose or substantial effect of obscuring, subverting or impairing a reasonable individual's autonomy, decision-making or choice.

"Data broker", a controller that, in a calendar year, knowingly collects and sells to third parties:

(i) the personal information of not less than 25,000 individuals; provided, however, that the controller derives not less than 25 per cent of its annual global gross revenues from the sale of personal information;

(ii) the biometric, genetic or specific geolocation information of not less than 10,000 individuals; or

(iii) 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: (A) customer, client, subscriber, user or registered user of the controller's goods or services; (B) an employee, contractor or agent of the controller; (C) an investor in the controller; or (D) 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 or 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", 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; provided, however, that the controller that possesses the information:

(i) takes reasonable technical and organizational measures to ensure that the information cannot, at any point, be associated with or used to re-identify an identified or identifiable individual or household;

(ii) publicly commits to process the information solely in a de-identified fashion;

(iii) does not attempt to re-identify the information; provided, however, that the controller may attempt to re-identify the information solely for the purpose of determining whether its de-identification procedures satisfy the provisions of this definition; and

(iv) contractually obligates any recipients of the information to comply with the provisions of this definition with respect to the information and requires that such obligations be included contractually in all subsequent instances for which the information may be received.

"De-identification", the creation of de-identified information from personal information.

"Designated method for submitting a request", a mailing address, email address, internet web page, internet web portal, toll-free telephone number or other applicable contact information through which an individual may submit a request or direction under this chapter.

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

"Genetic information", personal information, regardless of format, that:

(i) results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained; and

(ii) concerns an individual's genetic material including, but not limited to, deoxyribonucleic acids, ribonucleic acids, genes, chromosomes, alleles, genomes, alterations or modifications to deoxyribonucleic acids or ribonucelic acids, single nucleotide polymorphisms, uninterpreted data that results from analysis of the biological sample or other source or any information extrapolated, derived, or inferred therefrom.

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

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

"Health record", an individual's health-related record, as maintained pursuant to section 70 of said chapter 111.

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

"Homepage", 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 include:

(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; and

(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 household", 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", an individual who can be readily identified, directly or indirectly.

"Individual", 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", deriving information, data, assumptions, correlations, predictions or conclusions from facts, evidence or another source of information or data.

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

"Large data holder", a controller that, in a calendar year:

(i) has annual global gross revenues in excess of $1,000,000,000; and

(ii) determines the purposes and means of processing of the personal information of not less than 200,000 individuals, excluding personal information processed solely for the purpose of completing a payment-only credit, check or cash transaction where no personal information is retained about the individual entering into the transaction.

“Minor”, 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.

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

“Personal information”, information including, but not limited to, a unique persistent identifier, 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 publicly available or de-identified information about a natural person; and provided further, that “personal information” shall also include information including, but not limited to, a unique persistent identifier that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with:

(i) an identified or identifiable natural person, only insofar as “personal information” is used in clause (i) of the definition of “data broker” in this section; or

(ii) an identified or identifiable household, only insofar as “personal information” is used in: (i) subsection (b) of section 3; or (ii) any reference in this chapter to the sale or selling of personal information or the processing of personal information for the purposes of targeted cross-contextual or first-party advertising.

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

“Processor”, an entity that processes personal information on behalf of a controller; provided, however, that determining whether an entity is acting as a processor or a controller with respect to a specific processing of personal information is a fact-based determination that depends upon the context in which the information is processed; and provided further, that:

(i) a processor that continues to adhere to a controller’s instructions with respect to the specific processing of personal information remains a processor;

(ii) 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; and

(iii) 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.

“Profiling”, any form of automated processing of personal information to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual or household’s economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

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

"Publicly available information", information about an individual that:

(i) is lawfully made available from federal, state or local government records; or

(ii) a controller has a reasonable basis to believe is lawfully and intentionally made available to the general public: (A) through widely distributed media; or (B) by the individual, unless the individual has restricted the information to a specific audience; provided, however, that "publicly available information" shall not include biometric or genetic information or personal information that is not publicly available and has been combined with publicly available information.

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

"Sale" or "selling", disclosing, disseminating, making available, releasing, renting, sharing, 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 otherwise for the purposes of targeted cross-contextual advertising; provided, however, that "sale" or "selling" shall not include:

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

(ii) the controller’s use or sharing of an identifier for an individual who, pursuant to section 8, has opted out of the processing of the individual’s personal information; provided, however, that the controller’s use or sharing of the identifier is solely for the purpose of alerting entities that the individual has opted out;

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

(iv) 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;

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

(vi) when the individual uses or expressly directs the controller to disclose personal information to a third party or otherwise interact with a third party; provided, however, that the individual’s direction was not obtained through dark patterns; and provided further, that the controller’s interaction with the third party is not for the purposes of targeted cross-contextual advertising.

“Sensitive information”, a form of personal information, including:

(i) an individual’s specific geolocation information;

(ii) biometric or genetic information processed for the purpose of uniquely identifying an individual;

(iii) the personal information of a child or minor;

(iv) personal information that reveals an individual's: (A) racial or ethnic origin; (B) religious beliefs; or (C) citizenship or immigration status;

(v) personal information processed concerning an individual's past, present or future mental or physical health condition, disability, diagnosis or treatment;

(vi) personal information processed concerning an individual's sexual orientation, sex life or reproductive health including, but not limited to, the use or purchase of contraceptives, birth control, abortifacients or other medication related to reproductive health;

(vii) personal information that reveals an individual's philosophical beliefs or union membership;

(viii) personal information that reveals an individual's social security number, driver's license number, military identification number, passport number or state-issued identification card number; or

(ix) personal information that reveals an individual's 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.

"Specific geolocation information", 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 not greater than the area of a circle with a radius of 1,850 feet; provided, however, that "specific geolocation information" shall exclude 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 cross-contextual advertising", the targeting of advertising to an individual based on the individual's personal information obtained from the individual's activity across distinctly-branded internet websites, online applications, services or physical premises; provided, however, that "targeted cross-contextual advertising" shall not include:

(i) processing personal information solely for measuring or reporting advertising performance, reach or frequency;

(ii) contextual advertising that is displayed based on the content in which the advertisement appears and does not vary based on who is viewing the advertisement; or

(iii) advertising that is based solely on an individual's current intentional interaction with or visit to a controller's distinctly-branded internet website, online application, service or physical premise; provided however, that the individual's personal information is not: (A) used to build a profile about the individual or otherwise alter the individual's experience outside the current intentional interaction with the controller; or (B) retained after the completion of the interaction; provided further, that an individual's intentional interaction may include, but is not limited to, an individual's current search query or specific request for information and feedback; and provided further, that hovering over, muting, pausing or closing a given piece of content does not constitute an individual's intent to interact with a controller.

"Targeted first-party advertising", the targeting of advertising to an individual based on a controller profiling an individual by using the personal information obtained from the individual's activity within a controller's own websites, online applications, services or physical premises; provided, however, that “targeted first-party advertising” shall not include advertising or the processing of personal information pursuant to the exemptions specified in clauses (i) through (iii), inclusive, of the definition of targeted cross-contextual advertising.

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

“Trade secret” shall have the same meaning as defined in section 42 of chapter 93.

“Unique persistent identifier”, an identifier that is reasonably linkable to an identified or identifiable natural person or household including, but not limited to:

(i) a device identifier;

(ii) an Internet Protocol address;

(iii) a cookie;

(iv) a beacon;

(v) a pixel tag;

(vi) a mobile advertising identifier or similar technology;

(vii) a customer number;

(viii) a unique pseudonym;

(ix) a user alias;

(x) a telephone number; or

(xi) another form of persistent or probabilistic identifier that is linked or reasonably linkable to an identified or identifiable natural person or household.

"Upholding security, confidentiality and integrity", protecting against, responding to, preventing, detecting, investigating, reporting or prosecuting identity theft, fraud, harassment, malicious, deceptive or illegal activities, or any other security incidents that compromise the availability, authenticity, confidentiality or integrity of stored or transmitted personal information.

"Verifiable request", a request:

(i) to exercise any of the rights set forth in sections 10 through 13; 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 section 14.

Section 3. Scope and Applicability

(a) This chapter shall apply to:

(i) a controller or processor that conducts business in the commonwealth;

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

(iii) an entity that voluntarily certifies to the attorney general that it is fully in compliance with, and agrees to be bound by, this chapter.

(b) Notwithstanding subsection (a), sections 7 through 17, inclusive, and section 26 shall only apply to a controller that, during the preceding calendar year, satisfied 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, inclusive, and section 26 shall apply only to the personal information processed by the affiliate on behalf of the controller:

(1) The controller had annual global gross revenues in excess of 25,000,000 dollars;

(2) The controller was a data broker; or

(3) The controller determined the purposes and means of processing of the personal information of not less than 100,000 individuals, excluding personal information processed solely for the purpose of completing a payment-only credit, check or cash transaction where no personal information is retained about the individual entering into the transaction.

(c) This chapter shall not apply to:

(i) any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches or any political subdivision thereof;

(ii) a 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;

(iii) a registered futures association that is so designated pursuant to 7 U.S.C. 21, as amended from time to time; or

(iv) an entity that serves as a congressionally designated nonprofit, national resource center or clearinghouse to assist victims, families, child-serving professionals or the general public on issues concerning missing or exploited children.

(d) The following information shall be exempt from this chapter:

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

(ii) health records for the purposes of section 70 of chapter 111, to the extent that the records are maintained pursuant to 45 C.F.R. 160, 162 or 164;

(iii) information and documents that are created by a covered entity for purposes of complying with HIPAA;

(iv) information used only for public health activities or purposes as authorized by HIPAA;

(v) 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;

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

(vii) 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;

(viii) 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;

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

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

(xi) 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); or (C) a user of a consumer report, as set forth in 15 U.S.C. 1681b; provided, however, that this paragraph shall apply only to the extent that 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 the personal information is processed solely as authorized by the federal Fair Credit Reporting Act; and provided further, that the exemption established pursuant to this paragraph shall not apply with respect to section 26;

(xii) 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;

(xiii) 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;

(xiv) personal information processed in compliance with the federal Farm Credit Act, 12 U.S.C. 2001 et seq., as amended from time to time;

(xv) 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;

(xvi) personal information processed in compliance with chapter 175I;

(xvii) personal information processed by an air carrier specifically 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; provided, however, that this exemption shall apply solely to the extent that provisions of this chapter may be preempted by section 41713 of the Airline Deregulation Act; and

(xviii) personal information processed for purposes of chapter 176Q.

(e) Section 7 and sections 9 through 13, inclusive, shall not apply to information that is processed:

(i) in the course of an individual acting in a professional or commercial context, to the extent that the information is collected and used within that context;

(ii) 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 the individual's role;

(iii) as the emergency contact information of an individual acting pursuant to claus (ii) of this subsection, to the extent that the information is solely used for emergency contact purposes; or

(iv) in order to administer benefits for another natural person relating to an individual acting pursuant to clause (ii), to the extent that the information is used solely for the purposes of administering those benefits.

Section 4. Conflicting Provisions

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

(b) Controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act, 15 U.S.C. 6501 et seq., as amended from time to time, shall be in compliance with any obligation to obtain parental consent under this chapter. Nothing in this chapter shall be construed to relieve or change any obligations that a controller, processor or other entity may have under any such applicable federal law.

Section 5. General Principles for Processing Personal Information

(a) Personal information shall be:

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

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

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

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

(v) maintained in a form which permits identification of an individual for no longer than is necessary for the purposes for which the personal information is processed; and

(vi) processed in a manner that ensures that the information remains appropriately secure.

(b) A controller shall be responsible for complying with subsection (a) by implementing procedures that are reasonable and appropriate, taking into consideration:

(i) the size, scope and type of the controller;

(ii) the amount of resources available to the controller;

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

(iv) the need for upholding security, integrity and confidentiality with respect to the personal information processed by the controller.

(c) A controller that is compliant with the regulations promulgated pursuant to chapter 93H 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 clause (vi) of subsection (a) with respect to such personal information.

Section 6. Lawful Basis for Processing Personal Information

(a) Processing shall be lawful and in compliance with this chapter only if:

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

(ii) 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;

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

(iv) 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 the individual or other natural person is at risk or danger of death or serious physical injury; or

(v) 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; provided, however, that the controller shall conspicuously disclose such processing to the individual in advance and consider when assessing whether to process such personal information:

(A) the context in which the personal information would be collected;

(B) whether the processing is reasonably necessary and proportionate to provide or maintain a specific product or service requested or reasonably anticipated by the individual to whom the personal information pertains or to perform other specified purposes that are compatible with the reasonable expectations of the individual based on the individual's relationship with the controller;

(C) whether the controller or third party can achieve their legitimate interests in another, less intrusive, way;

(D) the amount of personal information that would be processed;

(E) the nature of the personal information that would be processed, taking into account whether processing the information, such as in the case of processing the business contact information of an individual acting in a commercial or business context, poses minimal risks to the individual;

(F) the possible unlawful disparate impacts and the financial, physical, reputational or other cognizable harms or consequences for the individual whose personal information would be processed;

(G) whether the processing interferes with an individual's right to privacy pursuant to section 1B of chapter 214; and

(H) the need for upholding security, integrity and confidentiality with respect to the personal information that would be processed.

(b) A controller shall not rely on clause (v) of subsection (a) as a lawful basis for processing personal information for the purposes of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the individual including, but not limited to, decisions that result in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

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:

(i) a clear and conspicuous description of: (A) whether the controller sells personal information to third parties or processes personal information for the purposes of targeted cross-contextual or first-party advertising; (B) what categories of sensitive information, if any, the controller processes and for what purposes; (C) an individual's rights pursuant to sections 8 through 13, inclusive; (D) how and where individuals may request to exercise these rights; and (E) a link to the attorney general's online mechanism through which the individual may contact the attorney general to submit a complaint pursuant to subsection (p) of section 25;

(ii) the categories of personal information processed by the controller;

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

(iv) the categories of personal information, if any, that the controller sells to third parties;

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

(vi) whether the controller sells personal information to registered data brokers, along with a link to the web page pursuant to clause (iii) of subsection (p) of section 25;

(vii) the affiliates to whom the controller discloses personal information;

(viii) the categories of sources from which personal information is collected;

(ix) 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, however, that a controller shall retain personal information for a duration consistent with clause (v) of subsection (a) of section 5;

(x) the effective date of the privacy notice;

(xi) whether or not any personal information processed by the controller is sold to, processed in, stored in or otherwise accessible to the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea or the Republic of Cuba; and

(xii) a contact method, such as an active email address or other online mechanism, that the individual may use to contact the controller.

(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 obligations 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) 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 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 clauses (i) through (ix), inclusive, of the definition of sensitive information under section 2.

(f) A large data holder shall retain and make publicly available on its internet website:

(i) copies of previous versions of its privacy notices for at least 10 years; and

(ii) a log describing the date and nature of each change to its privacy notice that is likely to affect a reasonable individual’s decision or conduct regarding a large data holder’s product or service.

(g) Subsection (f) shall only apply to privacy notices created or generated after the effective date of this section and shall not be retroactive.

Section 8. Opting Out of the Sale of Personal Information and Targeted Advertising

(a) An individual shall have the right to opt out of the processing of the individual's personal information for the purposes of:

(i) the sale of the personal information;

(ii) targeted cross-contextual advertising; or

(iii) targeted first-party advertising.

(b) A controller shall comply with an opt-out request pursuant to this section as soon as reasonably possible; provided, however, that a controller shall comply with an opt-out request with respect to clause (i) of subsection (a) in a time frame that is reasonably proportionate to the amount of time it takes the controller to sell such personal information to third parties; and provided further, that in any event, a controller shall comply with an opt-out request pursuant to this section not later than 15 days after receipt of the request.

(c) A controller that has received an opt-out request pursuant to this section shall be prohibited from processing the individual's personal information for the purposes of the sale of the personal information or for targeted cross-contextual or first-party advertising, as applicable, unless the individual subsequently provides consent for such processing. After complying with an individual's opt-out request, a controller shall wait for not less than 12 months before requesting the individual's consent to process the individual's personal information for the purposes of the sale of the personal information or for targeted cross-contextual or first-party advertising, as applicable.

(d) A data broker that has been sold an individual's personal information shall not further process an individual's personal information for the purposes of the sale of the personal information or for targeted cross-contextual advertising unless the individual has received explicit notice and is provided an opportunity to exercise the opt-out right pursuant to this section.

(e) If a controller communicates to any entity authorized by the controller to collect personal information that an individual has requested to exercise the opt-out right pursuant to this section, 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:

(i) processing the individual's personal information for the purposes of the sale of the personal information or for targeted cross-contextual or first-party advertising; and

(ii) processing that individual's personal information: (A) outside of the direct relationship between the entity and the controller; or (B) for any purpose other than for the specific purpose of providing or performing the services offered to the controller.

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

(g) An individual may designate an authorized agent to act on the individual's behalf to opt out of the processing of such individual's personal information for one or more of the purposes specified in subsection (a). The individual may designate such authorized agent by means including, but not limited to, a technology such as an internet link or a browser setting, browser extension or global device setting, indicating the individual’s intent to opt out of such processing. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the authorized agent’s authority to act on the individual’s behalf. An authorized agent shall:

(i) not use an individual’s personal information for any purposes other than to fulfill the individual’s requests, for verification or for fraud prevention; and

(ii) implement and maintain reasonable security procedures and practices to protect the individual’s personal information.

(h) A controller shall allow an individual to opt out of the processing of the individual’s personal information for one or more of the purposes specified in subsection (a) through an opt-out preference signal sent with the individual’s consent to the controller by a platform, technology or mechanism indicating the individual’s intent to opt out of such processing; provided, however, that such platform, technology or mechanism shall meet the requirements and technical specifications established by the attorney general pursuant to subsection (u) of section 25; and provided further, that a controller shall notify individuals about any such platform, technology or mechanism in any privacy notice provided pursuant to section 7.

(i) If an individual decides to opt out of the processing of the individual’s personal information for one or more of the purposes specified in subsection (a) through an opt-out preference signal sent in accordance with this chapter and the individual’s decision conflicts with the individual’s existing controller-specific privacy setting or voluntary participation in the controller’s bona fide loyalty, rewards, premium features, discounts or club card program, the controller shall comply with the individual’s opt-out preference signal but may notify the individual of the conflict and provide the individual with the choice to opt back into such controller-specific privacy setting or participation in such a program; provided, however, that the controller shall not use dark patterns to coerce the individual to opt back in to such controller-specific privacy setting or participation in such program.

(j) If a controller responds to an individual's opt-out request pursuant to this section by informing the individual of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered in accordance with section 16 for the collection, processing, sale or retention of the individual's personal information.

(k) A request to exercise the right to opt out pursuant to this section 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.

(l) For each calendar year in which a controller is a large data holder, the controller shall prepare a report that details the number of requests that is has received to opt out pursuant to clauses (i), (ii) and (iii) of subsection (a); provided, however, that the controller shall specify the number of such requests that the controller has denied; and provided further, that the controller shall make its report publicly available on its internet website and submit the report to the attorney general not later than January 31 following each year in which a controller meets the definition of a large data holder under this chapter.

Section 9. Protections for Sensitive Information

(a) A controller shall not process an individual’s sensitive information for the purposes of the sale of such information or for targeted cross-contextual or first-party advertising unless the controller has obtained the consent of the individual or, in the case of a child, the child’s parent or guardian.

(b) A controller shall not otherwise process an individual’s sensitive information without first obtaining the consent of the individual or, in the case of a child, the child’s parent or guardian, except to the limited extent necessary to:

(i) perform the services or provide the goods reasonably expected by an average individual who requests those services or goods;

(ii) maintain or service accounts, provide customer service, process or fulfill orders and transactions, verify customer information, process payments, provide financing, provide analytic services, provide storage or provide other similar services;

(iii) verify, maintain, improve or upgrade the quality or safety of the service or device that is owned, manufactured, manufactured for or controlled by the controller; or

(iv) perform short-term, transient use including, but not limited to, advertising that is based solely on an individual’s personal information derived from the individual’s current intentional interaction with the controller; provided, however, that the sensitive information shall not be an individual’s precise geolocation information; and provided further, that the individual’s sensitive information shall not be: (A) disclosed to another third party; or (B) used to build a profile about the individual or otherwise alter the individual’s experience outside the current interaction with the controller; or

(v) otherwise process the information pursuant to an exemption stipulated in section 24.

(c) If a controller does not receive consent for the processing of an individual's sensitive information, the controller shall wait for not less than 12 months before making a subsequent request for the individual or, in the case of a child, the child's parent or guardian, to consent to such processing.

Section 10. Right to Access and Transport Personal Information

(a) For the purposes of this section, "specific pieces of information" shall not include any data generated to uphold security, confidentiality and integrity.

(b) An individual shall have the right to request that a controller that processes the individual's personal information disclose to the individual the specific pieces of personal information that the controller has processed about the individual, including inferences linked or reasonably linkable to the individual.

(c) In response to a verifiable request pursuant to subsection (b), a controller shall provide to the individual the specific pieces of personal information that the controller has processed 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.

(d) The disclosure of the required information pursuant to this section 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; and provided further, that an individual's ability to request information beyond the 12-month period shall be disclosed in a controller's privacy notice pursuant to clause (i) of subsection (a) of section 7.

(e) 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 11. Right to Delete Personal Information

(a) An individual shall have the right to request that a controller delete any personal information processed about the individual.

(b) A controller that receives a verifiable request to delete the individual's personal information shall:

(i) delete the individual's personal information from its records;

(ii) notify all processors to whom the controller has disclosed the individual's personal information to delete the individual's personal information from their records; and

(iii) notify all third parties to whom the controller has sold the individual's personal information to delete the personal information from their records, unless doing so proves impossible or would constitute an undue burden for the controller.

(c) A controller may maintain a confidential record of deletion requests solely for:

(i) preventing the sale of the personal information of the individual who has submitted a deletion request;

(ii) ensuring that such individual's personal information is deleted from the controller's records; or

(iii) other purposes to the extent permissible pursuant to section 24 and subsection (i) of section 15.

(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:

(i) 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 the controller's ongoing relationship with the individual or otherwise perform a contract between the controller and the individual;

(ii) enable solely internal uses that are: (A) reasonably aligned with the expectations of the individual based on the individual's relationship with the controller; and (B) compatible with the context in which the individual provided the personal information;

(iii) maintain personal information that relates to a public figure and for which the individual making the deletion request has no reasonable expectation of privacy; or

(iv) comply with a legal obligation or otherwise process personal information pursuant to an exemption stipulated in section 24.

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

Section 12. Right to Correct Personal Information

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

Section 13. Right to Revoke Consent

(a) If a controller chooses to process an individual's personal information on the basis of the individual's consent pursuant to clause (i) of subsection (a) of section 6, the option for an individual to refuse consent shall be clear, at least as prominent as the option to accept and easy to use by a reasonable individual.

(b) In addition to an individual's opt-out right pursuant to section 8, an individual shall have the right to revoke consent that the individual previously gave to a controller to process the individual's personal information for any other purposes. The controller shall:

(i) provide a mechanism for individuals to revoke consent that is clear, conspicuous and easy to use by a reasonable individual; and

(ii) in response to an individual's verifiable request to revoke the individual's consent, cease to process the individual's personal information as soon as reasonably possible.

Section 14. Exercising Privacy Rights

(a) An individual may exercise the rights set forth in sections 8 through 13, inclusive, 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 child's parent or legal guardian may exercise the rights set forth in sections 8 through 13, inclusive, 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, the individual's guardian or conservator may exercise the rights set forth in sections 8 through 13, inclusive, on the individual's behalf.

Section 15. Responding to Requests to Exercise Privacy Rights

(a) Except as otherwise provided in this chapter, a controller shall comply with an individual's request to exercise the rights set forth in sections 10 through 13, inclusive.

(b) A controller shall inform the individual of any action taken on a request to exercise any of the rights set forth in sections 10 through 13, inclusive, 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; and provided further, that 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 10 through 13, inclusive, 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 section 14.

(d) A verifiable request to exercise the rights set forth in sections 10 through 13, inclusive, 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) When a controller, pursuant to section 23, is incapable of complying with an individual's verifiable request, the controller shall, if possible, notify the individual that it is unable to identify the individual and cannot act on the request. The individual, or a person entitled to exercise the rights of this chapter on behalf of the individual pursuant to section 14, may provide additional information to the controller enabling the individual's identification for the purposes of exercising the rights set forth in sections 10 through 13, inclusive.

(f) 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 (i). 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).

(g) A controller shall not be obligated to provide the information required by section 10 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.

(h) If requests from an individual, or from a person entitled to exercise the rights of this chapter on behalf of such individual pursuant to section 14, are manifestly unfounded, excessive or repetitive, the controller may: (i) charge a reasonable fee to cover the administrative costs of complying with the request; or (ii) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive nature of the request.

(i) 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 16. 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:

(i) denying goods or services to the individual;

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

(iii) providing a different level of quality of goods or services to the individual;

(iv) 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

(v) 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:

(i) the offering is in connection with an individual's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program; and

(ii) the difference is reasonably related to the value provided to the controller by the individual's personal information.

(c) Nothing in this section shall be construed to:

(i) require a controller to provide a product or service that requires an individual's personal information that the controller does not process; or

(ii) prohibit a controller from offering a financial incentive, including payments to individuals as compensation, for the processing of personal information; provided, however, that such payments shall be reasonably related to the value provided to the controller by the individual’s personal information.

Section 17. Disclosure of Methods for Exercising Privacy Rights

(a) A controller shall make available and describe in a privacy notice pursuant to section 7 not less than 2 designated methods for submitting a request to exercise the rights set forth in sections 8 through 13, inclusive. 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 whether the request is a verifiable request. If a controller maintains an internet website, the controller shall make its website available as 1 such designated method for submitting a request. A controller shall not require an individual to create a new account but may require an individual to use an existing account in order to exercise a right under this chapter.

(b) A controller that processes personal information for the purposes of selling such information or for targeted cross-contextual advertising shall 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 such processing.

(c) A controller that processes personal information for the purposes of targeted first-party advertising shall provide a clear and conspicuous link on the controller’s internet homepage to an internet web page that enables an individual, or an individual’s authorized agent, to exercise their right to opt out of such processing.

(d) In lieu of complying with both subsections (b) and (c), a controller that is subject to both 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 processing of the individual's personal information for the purposes of the sale of such information and for targeted cross-contextual and first-party advertising.

(e) A controller shall:

(i) ensure that all persons responsible for handling individuals' inquiries about the controller's privacy practices or compliance with this chapter are informed of: (A) all requirements set forth under this chapter; and (B) how to direct individuals to exercise their rights set forth in sections 8 through 13, inclusive;

(ii) 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;

(iii) process 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, inclusive, solely for the purposes of complying with the request;

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

(v) not require an individual to provide additional information beyond what is necessary to direct the controller, pursuant to section 8, to not process the individual's personal information for the purposes of the sale of such information or for targeted cross-contextual or first-party advertising; and

(vi) not condition, effectively condition, attempt to condition or attempt to effectively condition the exercise of the rights set forth in sections 8 through 13, inclusive, through the use of dark patterns or any false, fictitious, fraudulent or materially misleading statement or representation.

Section 18. No Waiver

Any provision of a contract or agreement 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 Among Controllers, Processors and Third Parties

(a) A processor shall not be required to comply with a request to exercise the rights set forth in sections 8 through 13, inclusive, 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.

(b) A processor shall adhere to the instructions of the controller and assist the controller in meeting its obligations under this chapter. Taking into account the nature of the processing and with respect to the personal information available to the processor as a result of its relationship with the controller, a processor shall:

(i) take appropriate technical and organizational measures, insofar as is possible, to fulfill the controller’s obligation to respond to individuals’ requests to exercise their rights pursuant to sections 8 through 13, inclusive;

(ii) provide information to the controller necessary to enable the controller to conduct and document any risk assessment required by section 21; and

(iii) 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; provided, however, that the controller and the processor shall: (A) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk; and (B) establish a clear allocation of the responsibilities between the processor and controller to implement such measures.

(c) When working with the controller to respond to a verifiable request to delete an individual’s personal information, the processor shall notify any processors or third parties who may have accessed the personal information from or through the processor to delete the personal information unless the information was accessed at the direction of the controller or doing so proves impossible or would constitute an undue burden.

(d) 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.

(e) 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 the provisions of subsection (f), that requires the entity to meet the obligations of the processor with respect to the personal information.

(f) A contract between a controller and a processor shall govern the processor's procedures with respect to processing individuals' personal information which 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:

(i) the nature and purpose of the processing;

(ii) the type of personal information subject to the processing;

(iii) the duration of the processing;

(iv) the rights and obligations of both parties;

(v) the requirements imposed by subsections (d) and (e); and

(vi) the following requirements:

(A) 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;

(B) 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;

(C) the processor shall allow for, and cooperate with, reasonable audits and inspections by the controller or the controller's designated auditor or 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, however, that the processor shall disclose a report of the audit to the controller upon request; and

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

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

(h) A controller shall exercise reasonable due diligence in:

(i) selecting a processor; and

(ii) deciding whether to sell personal information to a third party.

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 pay a registration fee of $200 and provide the following information:

(i) the data broker's name and primary physical, email and internet website addresses;

(ii) any privacy notice that the data broker discloses to individuals pursuant to section 7;

(iii) how individuals may request to exercise their rights under sections 8 through 13, inclusive;

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

(v) whether the data broker processes the personal information of minors or children;

(vi) whether it qualifies as a data broker pursuant to clause (i), (ii) or (iii) of the definition of a data broker under section 2;

(vii) whether the data broker is a large data holder; and

(viii) any additional information the data broker may wish to provide.

Section 21. Risk Assessments

(a) A controller shall establish, implement and maintain reasonable policies, practices and procedures to identify, assess and mitigate reasonably foreseeable privacy risks and cognizable harms related to their products and services, including the design, development and implementation of such products and services.

(b) A controller shall, prior to the processing, carry out and document a risk assessment of the impact of each of the following processing operations:

(i) processing personal information for the purposes of: (A) the sale of the personal information; (B) targeted cross-contextual advertising; or (C) targeted first-party advertising;

(ii) processing personal information for the purposes of profiling or otherwise systematically and extensively evaluating personal aspects relating to individuals; provided, however, that such processing presents a reasonably foreseeable risk of resulting in:

(A) discrimination on the basis of race, color, religion, national origin, sex or disability or other unfair or deceptive treatment of, or unlawful disparate impact on, individuals;

(B) financial, physical or reputational harm to individuals;

(C) 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

(D) other substantial cognizable harms to individuals;

(iii) processing sensitive information; and

(iv) any other processing that is likely to result in a high risk of harm to individuals, taking into account the nature, scope, context and purposes of the processing and whether the processing involves new technologies.

(c) The assessment shall contain at a minimum:

(i) 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;

(ii) a description and brief justification of the lawful basis, pursuant to section 6, that the controller is relying on to process the individual's personal information;

(iii) 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;

(iv) 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;

(v) a description of: (A) the context of the processing; (B) the relationship between the controller and the individual whose personal information would be processed; and (C) whether the controller is processing an individual's personal information in ways which the individual would reasonably expect;

(vi) an assessment of the risks of the processing operations to individuals; provided, however, that such assessment shall include, but not be limited to, whether the processing: (A) poses reasonably foreseeable risks to children or minors; (B) presents a reasonably foreseeable risk of disparate impact on the basis of individuals' race, color, religion, national origin, sex or disability; or (C) would result in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services; and

(vii) the measures envisioned to mitigate such risks including, but not limited to, safeguards such as de-identification and security measures to ensure the protection of personal information in compliance with this chapter, taking into account individuals' reasonable expectations of privacy or other legal rights.

(d) In any risk assessment required pursuant to this section, a large data holder shall also:

(i) specify whether the processing is based in whole or in part on an algorithmic computational process that:

(A) uses machine learning, natural language processing, artificial intelligence techniques or other techniques of similar or greater complexity;

(B) makes a decision or facilitates human decision-making with respect to personal information, including decisions that determine the provision of products or services or that rank, order, promote, recommend, amplify or similarly determine the delivery or display of information to an individual; or

(C) poses a reasonably foreseeable risk of substantial cognizable harm to individuals; and

(ii) include a description of:

(A) the design process and methodologies of any such algorithmic computational process pursuant to clause (i);

(B) the categories of data that would be processed as input or used to train the model that any such algorithmic computational process relies on; and

(C) the outputs that would be produced by any such algorithmic computational process.

(e) Subsections (a) through (d) shall not apply to processing:

(i) that a controller performs pursuant to clause(iii) of section 6; and

(ii) for which the controller has already carried out a risk assessment for the purpose of compliance with another applicable law that regulates the specific processing operation or set of operations in question; provided, however, that such assessment shall have reasonably comparable scope and effect to the assessment that would otherwise be conducted pursuant to this section.

(f) For the purpose of complying with this section, a controller may leverage its existing work product of risk assessments that the controller has conducted or is conducting for the purpose of complying with another applicable law.

(g) A single risk assessment may address a set of similar processing operations that present similar high risks.

(h) The controller shall carry out a review of the risk assessment if there is a change of the risk represented by the processing operations.

(i) A controller shall implement procedures to comply with this section that are reasonable and appropriate taking into consideration: (i) the size, scope and type of the controller; (ii) the amount of resources available to the controller; (iii) the amount and nature of personal information processed by the controller including, but not limited to, whether the personal information is sensitive information; and (iv) the need for upholding security, integrity and confidentiality with respect to the personal information processed by the controller.

(j) 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, who may evaluate the risk assessment for compliance with the responsibilities set forth in this chapter. Risk assessments shall be confidential and exempt from public inspection and copying under chapter 66. 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.

(k) Risk assessments shall apply to processing activities created or generated after the effective date of this section and shall not be retroactive.

Section 22. Processing That Unlawfully Discriminates

(a) A controller shall not process personal information in a manner that discriminates in, or otherwise makes unavailable, the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex or disability or other protected characteristic.

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

(c) Nothing in this section shall be construed to limit controllers from processing personal information for the purpose of:

(i) legitimate testing to prevent unlawful discrimination or otherwise determine the extent or effectiveness of the controller’s compliance with this section; or

(ii) diversifying an applicant, participant or customer pool.

(d) This section shall not apply to any private club or group not open to the public, pursuant to section 201(e) of the Civil Rights Act of 1964, 42 U.S.C. 2000a(e), as amended from time to time.

Section 23. De-Identified Information

This chapter shall not be construed to require a controller or processor, solely for the purpose of complying with this chapter, to:

(i) 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

(ii) reidentify or otherwise link de-identified information; provided, however, that the controller, pursuant to subsection (e) of section 15, shall provide applicable notice to the individual that it is unable to identify the individual.

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:

(i) comply with federal, state or local laws, rules or regulations;

(ii) comply with a civil, criminal or regulatory inquiry, subpoena or summons by federal, state, local or other governmental authorities;

(iii) 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;

(iv) investigate, establish, exercise, prepare for or defend legal claims.

(v) 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;

(vi) process the personal information of a child or minor solely to submit information relating to child victimization to law enforcement or to a nonprofit, national resource center or clearinghouse congressionally designated to provide assistance to victims, families, child-serving professionals or the general public on missing and exploited children issues; or

(vii) 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, inclusive, shall not restrict a controller or processor’s ability to process personal information for the following purposes, provided that the use of the individual’s personal information is reasonably necessary and proportionate for such purposes:

(i) helping to uphold security, confidentiality and integrity;

(ii) debugging to identify and repair errors that impair existing intended functionality;

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

(iv) 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 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 whether:

(A) 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) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

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

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

(ii) 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;

(iii) 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

(iv) 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.

(d) Personal information that is processed by a controller pursuant to an exemption under subsections (a) through (c) shall:

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

(ii) notwithstanding anything in this section to the contrary, be processed: (A) in accordance with section 5; and (B) subject to reasonable administrative, technical and physical measures to reduce reasonably foreseeable risks of harm to individuals.

(e) If a controller processes personal information pursuant to an exemption in subsections (a) through (c), inclusive, the controller shall demonstrate that such processing qualifies for such exemption and complies with the requirements of subsection (d).

(f) A controller or processor that discloses personal information to a processor or third party in compliance with the requirements of this chapter shall not be 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.

(g) A processor or third party receiving personal information from a controller or processor in compliance with the requirements of this chapter shall not be 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.

(h) 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 8 through 13, inclusive, 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:

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

(ii) compliance with the individual's request to exercise the rights set forth in sections 8 through 13, inclusive, would not be commercially reasonable; and

(iii) the controller complies with the individual's request as soon as it is commercially reasonable to do so, if applicable.

Section 25. Powers of the Attorney General

(a) Whenever the attorney general has reasonable cause to believe that an entity has engaged in, is engaging in or will imminently engage in a violation of this chapter, the attorney general may issue a civil investigative demand. The provisions of section 6 of chapter 93A 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, except as otherwise specified in section 26, shall not serve as the basis for or be subject to a private right of action under this chapter. Nothing in this chapter, except as otherwise specified in section 26, 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, 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 such further violations shall occur, the attorney general shall initiate no action against the entity.

(2) The cure period stipulated in 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: (A) this chapter; or (B) chapter 93A, provided that such violation occurred after the effective date of this section;

(ii) the attorney general and the entity have previously reached a settlement that includes an admission by the entity that it has violated: (A) this chapter, not including any express written statement provided pursuant to paragraph (1); or (B) chapter 93A, provided that such admission occurs after the effective date of this section;

(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; or

(v) the violation occurs more than 12 months after the effective date of this section and the violating entity is: (A) a large data holder; or (B) a data broker pursuant to clause (i) of the definition of a data broker under section 2.

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

(e)(1) The attorney general may initiate a civil action against an entity in the name of the commonwealth or as parens patriae on behalf of individuals if the entity:

(i) fails to cure a violation within 30 days after receipt of the attorney general's notice of the violation;

(ii) breaches an express written statement provided to the attorney general pursuant to subsection (d); or

(iii) is not eligible for a cure period pursuant to subsection (d).

(2) The attorney general may seek:

(i) civil penalties of up to $7,500 for each violation under this chapter; or

(ii) a temporary restraining order, preliminary injunction or permanent injunction to restrain any violations of this chapter.

(f) A data broker that fails to register as required by section 20 shall be subject to injunction and may be liable for civil penalties, fees and costs in a civil action brought on behalf of the commonwealth by the attorney general as follows:

(i) a civil penalty of up to $500 for each day, not to exceed a total of $100,000 for each year, that the data broker fails to register as required by section 20; and

(2) fees equal to the fees that would have been due during the period the data broker failed to register.

(g) The superior court shall have jurisdiction over 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.

(h) 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:

(i) the size, scope and type of the entity;

(ii) the amount of resources available to the entity;

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

(iv) the number of violations;

(v) the number of violations affecting children or minors;

(vi) the nature and severity of the violation;

(vii) the risks caused by the violation;

(viii) whether the entity’s violation was an isolated instance or part of a pattern of violations and noncompliance with this chapter;

(ix) whether the entity is a data broker that did not register pursuant to section 20;

(x) whether the violation was willful and not the result of error;

(xi) the length of time over which the violation occurred;

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

(xiii) the good faith cooperation of the entity with any investigations conducted by the attorney general pursuant to this section;

(xiv) efforts undertaken by the entity to cure the violation; and

(xv) the entity’s past violations of information privacy rules, regulations, codes, ordinances or laws in other jurisdictions.

(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 not more than $10,000 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, including attorney fees, incurred in investigating and preparing the case in any action initiated under this chapter.

(k) If 2 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 all to be 1 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:

(i) the number of written notices issued pursuant to subsection (c) and the number of entities that received such notices;

(ii) examples of alleged violations that have been cured by an entity pursuant to subsection (d); and

(iii) 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 will imminently engage in any violation of this chapter.

(p) The attorney general shall maintain the following internet web pages:

(i) 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;

(ii) a web page that enables data brokers to register pursuant to section 20; and

(iii) a web page that:

(A) makes publicly accessible the information provided by each data broker pursuant to section 20; provided, however, that the information shall be disaggregated by data broker; and

(B) includes a link and mechanism, if feasible, by which an individual may, pursuant to section 8, opt out of the processing of the individual's personal information by all registered data brokers for the purposes of the sale of such information or for targeted cross-contextual advertising or, pursuant to section 11, request that all registered data brokers delete any personal information processed about the individual.

(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, but not limited to, the rights of children and minors with respect to their own information. The attorney general shall provide guidance to individuals regarding available recourse if they believe their rights under this chapter have been violated.

(r) The attorney general shall create and make publicly accessible the following templates:

(i) a template privacy policy that is in compliance with section 7;

(ii) a template contract between a controller and a processor that is in compliance with section 19; and

(iii) a template risk assessment that is in compliance with section 21.

(s) The attorney general shall seek to collaborate with entities responsible for enforcing personal information privacy laws in other jurisdictions. The attorney general shall have the power to determine, pursuant to section 28, whether the provisions of a personal information privacy law in another jurisdiction are equally or more protective of personal information than the provisions of this chapter.

(t) The attorney general shall establish a mechanism pursuant to which an entity that processes the personal information of 1 or more individuals but does not meet the applicability criteria set forth in subsection (b) of section 3 may voluntarily certify that it is fully 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:

(i) 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 or privacy concerns;

(ii) ensuring that the notices and information that controllers are required to provide pursuant to section 7 are:

(A) provided in a manner that may be easily understood by the average individual;

(B) accessible to individuals with disabilities; and

(C) available in the language primarily used to interact with the individual;

(iii) detailing the requirements and technical specifications for a platform, technology or mechanism that sends an opt-out preference signal indicating an individual's intent to opt out of the processing of such individual's personal information for 1 or more of the purposes specified in subsection (a) of section 8; provided, however, that such requirements or technical specifications shall be updated from time to time to reflect the means by which individuals interact with controllers; and provided further, that any such platform, technology or mechanism shall:

(A) not unfairly disadvantage another controller;

(B) clearly represent the individual's affirmative, freely-given and unambiguous intent to opt out pursuant to subsection (a) of section 8 and be free of default settings constraining or presupposing that intent;

(C) be consumer-friendly, clearly described and easy to use by the average individual;

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

(E) enable the controller to accurately determine if the mechanism represents a legitimate opt-out request pursuant to section 8; and

(iv) supplementing or revising the list of industry recognized cybersecurity frameworks specified in clauses (i) and (ii) of subsection (d) of section 26, in order to address changes in technology, data collection, obstacles to implementation, best practices with respect to cybersecurity controls or privacy concerns.

(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 by the federal government or other states, territories or countries. Specific topics for research shall include, but are not limited to:

(i) the available best methods for: (A) individuals to exercise the rights set forth in sections 8 through 13, inclusive; and (B) entities to conspicuously and clearly disclose how to exercise such rights;

(ii) automated decision-making technologies;

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

(iv) financial incentive programs offered by controllers for the processing of personal information;

(v) the data broker industry, including data brokers that have registered pursuant to section 20;

(vi) the effectiveness of allowing an individual to designate an authorized agent to exercise a right on their behalf pursuant to section 8; and

(vii) whether to change or eliminate the cure period established in subsection (d) of section 25.

(w) Every 12 months, the attorney general shall provide a full written report to the joint committee on advanced information technology, the internet and cybersecurity. The report shall summarize the attorney general's work pursuant to this section and detail the attorney general's research and any recommendations with respect to privacy-related legislation. The first such report shall be submitted 12 months after the effective date of this subsection.

(x) Monetary amounts referred to in this chapter shall be indexed biennially 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. Private Right of Action and Safe Harbor

(a) For the purposes of this section, except for the purposes of determining whether this section applies to a given controller, the terms "breach of security" and "personal information" shall have the same meanings as such terms are defined in section 1 of chapter 93H.

(b) Any individual whose personal information is subject to a breach of security 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:

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

(ii) injunctive or declaratory relief; or

(iii) any other relief the court deems proper.

(c) In determining the amount of statutory damages against the controller, the court shall consider any 1 or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the criteria stipulated in clauses (i) through (xv), inclusive, of subsection (h) of section 25.

(d) 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 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; provided, however, that the controller designed and implemented its cybersecurity program in accordance with the regulations adopted pursuant to chapter 93H; and provided further, that:

(i) such cybersecurity program conforms to the current version of or any combination of the current versions of:

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

(B) the National Institute of Standards and Technology’s special publication 800-171;

(C) the National Institute of Standards and Technology’s special publications 800-53 and 800-53a;

(D) the Federal Risk and Authorization Management Program’s “FedRAMP Security Assessment Framework”;

(E) the Center for Internet Security’s “Center for Internet Security Critical Security Controls for Effective Cyber Defense”; or

(F) the “ISO/IEC 27000-series” information security standards published by the International Organization for Standardization and the International Electrotechnical Commission; or

(ii) such 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 clause (i).

(e) When a revision to a document listed in clause (i) or (ii) of subsection (d) 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 6 months after the publication date of the revision.

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

(i) the size, scope and type of the controller;

(ii) the amount of resources available to the controller;

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

(iv) the need for upholding security, integrity and confidentiality with respect to the personal information processed by the controller.

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

(h) Nothing in this section shall limit the authority of the attorney general to initiate actions pursuant to:

(i) section 25 of this chapter;

(ii) chapter 93A or 93H; or

(iii) any other general law.

(i) The cause of action established by this section shall apply only to violations as defined in this section.

Section 27. Massachusetts Privacy Fund

(a) There shall be established upon the books of the commonwealth a separate 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 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 remain in the fund and not revert to the General Fund.

(c) The attorney general shall have discretion to allocate the proceeds of any settlement of a civil action pursuant to this chapter to:

(i) the Massachusetts Privacy Fund;

(ii) the General Fund; or

(iii) 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. Moneys in the fund shall be subject to appropriation and shall not be used to supplant General Fund appropriations to the attorney general.

Section 28. Reciprocity and Interoperability

(a) A controller or processor shall be in compliance with provisions of this chapter if:

(i) the controller or processor complies with comparable provisions of a personal information privacy law in another jurisdiction;

(ii) the controller or processor applies the provisions of that law to its processing activities concerning individuals; and

(iii) 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 such law are equally or more protective than the provisions of this chapter.

Section 29. Implementation for Nonprofits and Institutions of Higher Education

This chapter shall apply to nonprofit organizations and institutions of higher education.

SECTION 2. Except as otherwise provided herein, chapter 93M of the General Laws, as inserted by section 1, shall take effect 18 months after the passage of this act; provided, however, that:

(i) section 2 and subsections (p) through (w), inclusive, of section 25 of said chapter 93M shall take effect upon enactment; and

(ii) section 30 of said chapter 93M shall take effect 30 months after enactment.