HOUSE . . . . . No. 4746

The Commonwealth of Massachusetts

HOUSE OF REPRESENTATIVES, November 17, 2025.

The committee on Advanced Information Technology, the Internet and Cybersecurity, to whom was referred the petition (accompanied by bill, House, No. 78) of Tricia Farley-Bouvier and others for legislation to establish the Massachusetts consumer data privacy act; the petition (accompanied by bill, House, No. 80) of Kate Hogan and Lindsay N. Sabadosa for legislation to establish a comprehensive consumer data privacy act; the petition (accompanied by bill, House, No. 86) of Kate Lipper-Garabedian, David T. Vieira and others relative to regulation of location information derived from electronic devices; the petition (accompanied by bill, House, No. 96) of David M. Rogers and Andres X. Vargas relative to the use of biometric recognition technology; the petition (accompanied by bill, House, No. 103) of Andres X. Vargas and Simon Cataldo for legislation to establish the Massachusetts neural data privacy protection act; and the petition (accompanied by bill, House, No. 104) of Andres X. Vargas, David M. Rogers and others for legislation to establish the Massachusetts data privacy act, reports recommending that the accompanyingbill (House, No. 4746) ought to be pass.

For the committee,

TRICIA FARLEY-BOUVIER.

FILED ON: 11/12/2025

HOUSE . . . . . No. 4746

The Commonwealth of Massachusetts

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

An Act establishing the Massachusetts consumer data privacy act.

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

SECTION 1. The General Laws, as appearing in the 2024 Official Edition, are hereby amended by inserting after chapter 93L the following chapter:

Chapter 93M. Massachusetts Consumer Data Privacy Act

Section 1. Definitions.

As used in this chapter, unless the context otherwise requires:

"Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity. For the purposes of this definition, "control" and "controlled" mean:

(i) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company;

(ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

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

"Affirmative Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a controller, provided that:

(i) the request is provided to the consumer in a clear and conspicuous stand-alone disclosure;

(ii) the request includes a description of the processing purpose for which the consumer's consent is sought and:

(A) clearly distinguishes between an act or practice that is necessary to fulfill a request of the consumer and an act or practice that is for another purpose;

(B) clearly states the specific categories of personal data that the controller intends to collect, process, transfer, or sell under each act or practice; and

(C) is written in easy-to-understand language and includes a prominent heading that would enable a reasonable consumer to identify and understand each act or practice;

(iii) the request clearly explains the consumer's rights related to consent;

(iv) the request is made in a manner reasonably accessible to and usable by consumers with disabilities;

(v) the request is made prior to the controller's implementation of the act or practice;

(vi) the request is made available to the consumer in each language in which the controller provides a product or service for which authorization is sought;

(vii) the option to refuse to give consent is at least as prominent as the option to give consent and the option to refuse to give consent takes the same number of steps or fewer as the option to give consent; and

(viii) affirmative consent to an act or practice is not inferred from the inaction of the consumer or the consumer's continued use of a service or product provided by the controller.

“Affirmative Consent” does not include:

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

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

(iii) agreement obtained through the use of a false, fraudulent, or materially misleading statement or representation; or

(iv) agreement obtained through the use of dark patterns.

“Authenticate” means to use reasonable means to determine that a request to exercise any of the rights afforded under this chapter is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

“Biometric data” means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, gait, or other unique biological patterns or characteristics that can be used to identify a specific individual.

“Biometric data” does not include:

(i) a digital or physical photograph,

(ii) an audio or video recording, or

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

“Browser” means an interactive software application that is primarily used by consumers to access internet websites.

“Business associate” has the same meaning as provided in HIPAA.

“Child” has the same meaning as provided in COPPA.

“Collect” means buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring personal data by any means.

“Consumer” means an individual who is a resident of this state. “Consumer” does not include an individual acting as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

“Consumer health and wellness data” means personal data that is collected by a health and wellness device or application that is not otherwise biometric data, neural data, genetic data or personal data that reveals a mental or physical health condition, diagnosis, disability, or treatment.

"Contextual advertising” means displaying or presenting an advertisement that does not vary based on the identity of the individual recipient and is based solely on—

(i) the immediate content of a webpage or online service within which the advertisement appears; or

(ii) a specific request of the consumer for information or feedback if displayed in proximity to the results of such request for information;

Provided, however, that a controller may use the following types of personal data to display a contextual advertisement so long as the personal data is not used to make inferences about the consumer, profile the consumer, or for any other purpose, and that the consumer may use technical means to obfuscate or change their physical location and to specify a language preference —

(i) such technical specifications as are necessary for the ad to be delivered and display properly on a given device;

(ii) a consumer's immediate presence in a geographic area with a radius no smaller than 10 miles, or an area reasonably estimated to include online activity from at least 5,000 users, but not including precise geolocation data; or

(iii) the consumer's language preferences, as inferred from context, browser settings, or user settings.

"Controller" means a person who, alone or jointly with others, determines the purpose and means of collecting or processing personal data.

"COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

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

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

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

"De-identified data" means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data:

(i) takes reasonable physical, administrative, and technical measures to ensure that such data cannot be associated with an individual or be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual,

(ii) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and

(iii) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (i) and (ii) of this definition.

"First party" means a consumer-facing controller with which the consumer intends or expects to interact.

"First-party advertising" means processing by a first party of its own first-party data for the purposes of advertising and marketing and carried out—

(i) through direct communications with a consumer, such as direct mail, email, or text message communications;

(ii) in a physical location operated by the first party; or

(iii) through display or presentation of an advertisement on the first party's own website, application or its other online content.

"First-party advertising" includes marketing measurement related to such advertising and marketing.

"First-party data" means personal data collected directly from a consumer by a first party, including based on a visit by the consumer to or use by the consumer of a website, a physical location, or an online service operated by the first party.

"Gender-affirming health care services" shall have the same meaning as defined in section 11I ½ of chapter 12.

"Gender-affirming health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services.

"Genetic data" means any data, regardless of its format, that concerns an individual's genetic characteristics, including, but not limited to raw sequence data that results from the sequencing of the complete, or a portion of the, extracted deoxyribonucleic acid of an individual or any genotypic and phenotypic information that results from analyzing such raw sequence data.

"Health and wellness device or application" means a device or application that is designed to allow a consumer to track or monitor information regarding the consumer's health and wellness, including but not limited to fitness, nutrition, diet, physical activity, sleep, mental state, stress, or behavior, either retroactively or in real time;

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

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

"Large data holder" means a controller or processor that in the most recent calendar year:

(i) had annual gross revenues of $200,000,000 or more; and

(ii) collected, processed, or transferred the covered data of more than 2,000,000 consumers or devices that identify or are linked or reasonably linkable to one or more consumers, excluding covered data collected and processed solely for the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested product or service; or the sensitive covered data of more than 200,000 consumers or devices that identify or are linked or reasonably linkable to one or more consumers.

The term "large data holder" does not include any instance in which the controller or processor would qualify as a large data holder solely on the basis of collecting or processing personal email addresses, personal telephone numbers, or log-in information of an individual or device to allow the individual or device to log in to an account administered by the controller or processor.

"Legally-protected health care activity" shall have the same meaning as defined in section 11I ½ of chapter 12.

"Legally-protected health care data" means any personal data concerning any effort made by a consumer to seek, or a consumer's receipt of, legally-protected health care activity.

"Marketing measurement" means measuring and reporting on marketing performance or media performance by the controller, including processing personal data for measurement and reporting of frequency, attribution, and performance.

"Minor" means any individual who is younger than 18 years of age.

"Neural data" means information that is generated by measuring the activity of an individual's central or peripheral nervous system.

"Person" means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust or other legal entity.

"Personal data" means any information, including derived data and unique identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or a device that identifies or is linked or reasonably linkable to an individual. "Personal data" does not include de-identified data or publicly available information.

"Precise geolocation data" means information derived from technology, including, but not limited to, latitude and longitude coordinates from global positioning system mechanisms or other similar positional data, that reveals the past or present physical location of an individual or

device that identifies or is linked or reasonably linkable to 1 or more individuals with precision and accuracy within a radius of 1,750 feet.

"Precise geolocation data" does not include the content of communications, a photograph or video, metadata associated with a photograph or video that cannot be linked to an individual, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

"Process" means to perform any operation or set of operations , whether by manual or automated means, on personal data or on sets of personal data, such as the use, storage, disclosure, analysis, deletion or modification of personal data.

"Processor" means a person who collects, processes, or transfers personal data on behalf of, and at the direction of, a controller or another processor, or a Federal, State, Tribal, or local government entity.

"Profiling" means any form of processing performed on personal data to evaluate, analyze or predict personal aspects including an individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

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

"Publicly available information" means information that has been lawfully made available to the general public from:

(i) federal, state or municipal government records, if the person collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity;

(ii) widely distributed media; or

(iii) a disclosure to the general public as required by federal, state, or local law.

"Publicly available information" does not include:

(i) Any obscene visual depiction, as defined in section 1460 of title 18, United States Code;

(ii) any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive data with respect to a consumer;

(iii) biometric data;

(iv) personal data that is created through the combination of personal data with publicly available information;

(v) genetic or neural data, unless otherwise made publicly available by the individual to whom the information pertains;

(vi) information made available by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has restricted the information to a specific audience; or

(vii) intimate images, authentic or computer-generated, known to be nonconsensual, including, but not limited to, images distributed in violation of section 43A of chapter 265.

"Reproductive or sexual health care" means any health care-related services or products rendered or provided concerning a consumer's reproductive system or sexual well-being,

including, but not limited to, reproductive health care services as defined in section 11I ½ of chapter 12 or any such service or product rendered or provided concerning

(i) an individual's health condition, status, disease, diagnosis, diagnostic test or treatment,

(ii) a social, psychological, behavioral or medical intervention,

(iii) a surgery or procedure, including, but not limited to, an abortion,

(iv) a use or purchase of a medication, including, but not limited to, a medication used or purchased for the purposes of an abortion,

(v) a bodily function, vital sign or symptom,

(vi) a measurement of a bodily function, vital sign or symptom, or

(vii) an abortion, including, but not limited to, medical or nonmedical services, products, diagnostics, counseling or follow-up services for an abortion.

"Reproductive or sexual health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

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

"Sale of personal data" does not include:

(i) the disclosure of personal data to a processor that processes the personal data on behalf of the controller;

(ii) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

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

(iv) with the consumer's affirmative consent, the disclosure of personal data where the consumer affirmatively directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; or

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

(vi) the disclosure of personal data that the consumer:

(A) intentionally made available to the general public via a channel of mass media; and

(B) did not restrict to a specific audience.

"Sensitive data" means personal data that includes:

(i) data revealing a consumer's (A) racial or ethnic origin, color, national origin or citizenship or immigration status; (B) religious beliefs; (C) mental or physical health condition, diagnosis, disability or treatment, including, but not limited to, gender-affirming health data, reproductive or sexual health data or legally-protected health care data; (D) sex life, sexual orientation, status as transgender or non-binary; (E) union membership; (F) status as a victim of a crime; or (G) status as a military servicemember or veteran;

(ii) consumer health and wellness data;

(iii) genetic, neural, or biometric data;

(iv) personal data of a consumer that a controller knows, or willfully disregards, is a minor;

(v) precise geolocation data;

(vi) a government-issued identifier, including a Social Security number, passport number or driver's license number, that is not required by law to be displayed in public; or

(vii) account names, passwords, usernames, access codes, security questions or answers, or other credentials and information used to log in to an account or device.

“Targeted advertising” means displaying or presenting an online advertisement to a consumer or to a device identified by a unique persistent identifier (or to a group of consumers or devices identified by unique persistent identifiers), if the advertisement is selected based, in whole or in part, on known or predicted preferences, characteristics, behavior, or interests associated with the consumer or a device identified by a unique persistent identifier.

“Targeted advertising” includes displaying or presenting an online advertisement for a product or service based on the previous interaction of a consumer or a device identified by a unique persistent identifier with such product or service on a website or online service that does not share common branding with the website or online service displaying or presenting the advertisement, and marketing measurement related to such advertisements.

“Targeted advertising” does not include:

(i) first-party advertising; or

(ii) contextual advertising.

"Third party" means a person that collects personal data from another person that is not the consumer to whom the data pertains and is not a processor with respect to such data.

"Third party" does not include a person that collects personal data from another entity if the two entities are affiliates.

"Trade secret" has the same meaning as provided in section 42 of chapter 93.

"Transfer" means to disclose, release, disseminate, make available, license, rent, or share personal data to a third party orally, in writing, electronically, or by any other means.

"Unique persistent identifier" means a technologically created identifier to the extent that such identifier is reasonably linkable to a consumer or a device that identifies or is linked or reasonably linkable to 1 or more consumers, including device identifiers, Internet Protocol addresses, cookies, beacons, pixel tags, mobile ad identifiers or similar technology customer numbers, unique pseudonyms, user aliases, telephone numbers, or other forms of persistent or probabilistic identifiers that are linked or reasonably linkable to 1 or more consumers or devices.

The term "unique persistent identifier" does not include an identifier assigned by a controller for the sole purpose of giving effect to the exercise of affirmative consent or opt out by a consumer with respect to the collecting, processing, and transfer of personal data or otherwise limiting the collecting, processing, or transfer of personal data.

Section 2. Applicability.

The provisions of this chapter apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year:

(a) Collected or processed the personal data of not less than 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction, so long as all personal data collected or processed for such purpose was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a business's return policy;

(b) derived gross revenue from the sale of personal data; or

(c) collected or processed sensitive data.

Section 3. Scope.

(a) The provisions of this chapter, except for the provisions of paragraph (4) of subsection (a) of section 6, do not apply to:

(1) any Federal, State, Tribal, territorial, or local government entity such as a body, authority, board, bureau, commission, district or agency of the Commonwealth or of any political subdivision of the Commonwealth;

(2) a nonprofit organization established to detect and prevent fraudulent acts in connection with insurance that is operating solely for that purpose;

(3) a national securities association registered pursuant to section 15A of the Securities Exchange Act of 1934 and the rules and implementing regulations promulgated thereunder;

(4) a registered futures association designated pursuant to section 17 of the Commodity Exchange Act and the rules and implementing regulations promulgated thereunder;

(5) a bank, credit union or any affiliate or subsidiary thereof that: (A) is only and directly engaged in financial activities as described in 12 USC 1843(k); (B) is regulated and examined by the division of banks or an applicable federal bank regulatory agency; and (C) has established a program to comply with all applicable requirements established by the commissioner of banks or the applicable federal bank regulatory agency concerning personal data; or

(6) an agent, broker-dealer, investment adviser or investment adviser representative, as defined in section 401 of chapter 110A, who is regulated by the secretary of the commonwealth or the United States Securities and Exchange Commission.

(b) The following information and data is exempt from the provisions of this chapter:

(1) protected health information that a covered entity or business associate collects or processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with HIPAA and regulations promulgated under HIPAA, as in effect on the effective date of this Act;

(2) patient-identifying information for purposes of 42 USC 290dd-2;

(3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46;

(4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the

International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;

(5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law;

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

(7) patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time;

(8) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

(9) personal information collected, processed, or sold subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.;

(10) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time;

(11) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time;

(12) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time;

(13) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time;

(14) data collected, processed, or maintained:

(i) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role;

(ii) as the emergency contact information of an individual under this chapter used for emergency contact purposes; or

(iii) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under paragraph (1) of this subsection and used for the purposes of administering such benefits; and

(15) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Federal Aviation Act of 1958, 49 USC 40101 et seq., to the extent this chapter is preempted by the Federal Aviation Act of 1958, and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

(c) Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to this chapter.

Section 4. Consumer rights.

(a) A consumer shall have the right to:

(1) Confirm whether or not a controller is collecting or processing the consumer's personal data and access such personal data, including, but not limited to, any inferences about the consumer derived from such personal data;

(2) obtain from a controller a list of specific third parties, other than natural persons, to which the controller has transferred either (i) the consumer’s personal data; or (ii) any personal data;

(3) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data, and instruct a controller or processor to make reasonable efforts to notify all third parties or processors to which the controller has transferred such personal data of such corrections;

(4) delete personal data provided by, or obtained about, the consumer, including personal data the consumer provided to the controller, personal data the controller obtained from another source, and derived data and instruct a controller or processor to make reasonable efforts to notify all third parties or processors to which the controller has transferred such personal data of such deletion request;

(5) obtain a copy of the consumer's personal data collected or processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and

(6) opt out of the collection and processing of the consumer’s personal data for purposes of:

(i) targeted advertising;

(ii) the sale of personal data; or

(iii) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(b) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 5 of this act to exercise the rights of such consumer specified in this section on behalf of the consumer. In the case of personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

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

(1) A controller shall respond to the consumer without undue delay, but not later than 45 days after receipt of the request. The controller may extend the response period by 20 additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial 45-day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, not less than twice per consumer during any twelve-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under paragraphs (1) to (5), inclusive, of subsection (a) of this section using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights, provided that any such information may not be used for

any purposes other than the authentication of such consumer. A controller shall not require authentication to exercise an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to paragraph (4) of subsection (a) of this section by deleting the consumer’s personal data retained by the controller and retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose pursuant to this chapter.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than 60 days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

(e) A controller may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a right described in this section through—

(1) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(2) the use of dark patterns.

(f) A controller or processor may not collect, process, or transfer personal data in a manner that discriminates against an individual or class of individuals, or otherwise makes unavailable the equal enjoyment of goods or services, on the basis of an individual's or class of individuals' actual or perceived race, color, sex, sexual orientation, gender identity, disability, religion, genetic information, pregnancy or condition related to pregnancy, status as a veteran, ancestry or national origin, or any other basis protected by chapter 151B.

(g) Subsection (f) does not apply to:

(1) The collection, processing, or transfer of personal data for the sole purpose of:

(i) A controller or processor's self-testing to prevent or mitigate unlawful discrimination or otherwise to ensure compliance with state or federal law; or

(ii) Diversifying an applicant, participant or customer pool; or

(2) A private establishment, as described in 42 United States Code, Section 2000a(e).

Section 5. Authorized agent.

A consumer may designate another person to serve as the consumer's authorized agent, and act on such consumer's behalf, to exercise rights specified in subsection (a) of section 4 of

this act. A controller shall comply with a request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf.

Section 6. Actions of controllers.

(a) A controller shall:

(1) limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains, including any routine administrative, operational, or account-servicing activity, such as billing, shipping, delivery, storage, accounting, or sending communications;

(2) not process or transfer personal data concerning a consumer in a manner that is inconsistent with the reasonable expectations of the consumer;

(3) not collect, process, or transfer sensitive data concerning a consumer except when such collection, processing, or transfer is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains;

(4) not sell:

(i) precise geolocation data regarding a consumer; or

(ii) sensitive data other than precise geolocation data regarding a consumer without obtaining the consumer’s affirmative consent;

(5) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data

appropriate to the volume and nature of the personal data at issue, including disposing of personal data in accordance with a retention schedule that requires the deletion of personal data when the data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected, processed, or transferred;

(6) not transfer or sell sensitive data concerning a consumer without obtaining the consumer's affirmative consent, or, in the case of the collection or processing of personal data concerning a known child, without collecting or processing such data in accordance with COPPA;

(7) provide an effective mechanism for a consumer to revoke the consumer's affirmative consent under this chapter that is at least as easy as the mechanism by which the consumer provided the consumer's affirmative consent and, upon revocation of such affirmative consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request;

(8) not collect or process the personal data of a consumer for purposes of targeted advertising or first-party advertising, or sell the consumer's personal data, under circumstances where a controller has actual knowledge, or willfully disregards, that the consumer is a minor; and

(9) not discriminate or retaliate against a consumer for exercising any of the consumer rights contained in this chapter, or for refusing to agree to the collection or processing of personal data for a separate product or service, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.

(b) Nothing in paragraph (9) of subsection (a) shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, club card, or similar program, provided that:

(1) the controller may not transfer personal data to a third party as part of such program unless such transfer is clearly and conspicuously disclosed in the terms of the program; and

(2) the sale of personal data shall not be a condition of participation in the program.

A controller shall not use financial incentive practices that are unjust, unreasonable, coercive or usurious in nature.

(c) A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes:

(1) The categories of personal data collected and processed by the controller, including a separate list of categories of sensitive data collected and processed by the controller, described in a level of detail that provides consumers a meaningful understanding of the type of personal data collected or processed;

(2) the purpose for collecting and processing each category of personal data the controller collects or processes described in a way that gives consumers a meaningful understanding of how each category of their personal data will be used;

(3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) the categories of personal data that the controller transfers to third parties, if any, and the purposes for those transfers;

(5) the categories of third parties, if any, to which the controller transfers personal data;

(6) The length of time the controller intends to retain each category of personal data, or, if it is not possible to identify the length of time, the criteria used to determine the length of time the controller intends to retain categories of personal data; and

(7) an active electronic mail address or other online mechanism that the consumer may use to contact the controller.

The privacy notice shall be provided directly to consumers and made available online to the general public. If a controller makes a material change to its privacy notice, the controller shall notify each consumer affected by the material change before implementing the material change with respect to prospectively collected personal data and provide a reasonable opportunity for each consumer to withdraw consent. A controller should provide a reasonable opportunity for each consumer to affirmatively consent to further materially different processing or transfer of previously collected personal data under the changed policy. The controller shall take all reasonable electronic measures to provide direct notification regarding material changes to the privacy notice to each affected consumer, taking into account available technology and the nature of the relationship.

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

(e) A controller shall establish, and shall describe in a privacy notice, not less than two secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. Any such means shall include:

(1) Providing a clear and conspicuous link on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising, the sale of the consumer's personal data, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer; and

(2) Not later than 18 months after the effective date of this chapter, allowing a consumer to opt out of any collection or processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the consumer’s personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the

controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall:

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

(ii) Enable the controller to reasonably determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising. For purposes of this subsection, the use of an internet protocol address to estimate the consumer’s location shall be considered sufficient to reasonably determine residency.

If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of personal data, through an opt-out preference signal sent in accordance with the provisions of this subsection conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's financial incentive program, the controller shall comply with such consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program.

(f) If a controller responds to consumer opt-out requests received pursuant to subsection (e) of this section by informing the consumer of a change in the price, rate, level, quality, or selection of goods or services, the controller shall present the terms of any financial incentive offered pursuant to subsection (b) of this section for the processing, sale or transfer of the consumer's personal data.

(g) For the purposes of paragraphs (1) and (3) of subsection (a), “requested by the consumer” shall not be construed to require an express or written request for a product or service

prior to the collection, processing or transfer of a consumer's personal data. A controller shall determine that a consumer is requesting a product or service based on objective circumstances that indicate that a consumer is seeking such product or service, including, but not limited to, (i) whether the consumer has registered for, downloaded or otherwise deliberately used an account, application, service or website, (ii) the consumer's relationship with the controller and (iii) the manner in which such product or service is customarily delivered or rendered in the ordinary course of business. A controller may draw inferences as is reasonably necessary based upon such objective circumstances, provided, however, that inferences shall not be drawn in a manner inconsistent with the reasonable expectations of the consumer.

(h) For the purposes of subsection (g) and paragraph (2) of subsection (a), the "reasonable expectations of the consumer" shall be based on the following: (i) the relationship between the consumer and the controller; (ii) the type, nature, and amount of personal data that the controller seeks to collect; (iii) the source of the personal data and the controller's method for collecting it; (iv) the specificity and clarity of information provided to the consumer about the purpose for collecting their personal data; (v) the degree to which the involvement of processors and third parties in the collecting or processing of personal data is apparent to the consumer.

Section 7. Responsibilities of processors and controllers.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter. Such assistance shall include:

(1) taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests;

(2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor, in order to meet the controller's obligations; and

(3) providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be written, binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties including a method by which the processor shall notify the covered entity of material changes to its privacy practices. The processor shall adhere to the instructions of the controller and only process and transfer the data it receives from the controller to the extent necessary to provide a service requested by the controller, as set out in the contract. The contract shall also require that the processor:

(1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

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

(3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

(4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the contractual and statutory or regulatory obligations of the processor with respect to the personal data;

(5) be prohibited from combining personal data that the processor receives from or on behalf of a controller with personal data that the processor receives from or on behalf of another person or collects from the interaction of the processor with an individual; and

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

(c) A processor shall establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data that are consistent with chapter 93H and appropriate to the volume and nature of the personal data at issue.

(d) Nothing in the contract in subsection (b) shall relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in this chapter.

(e) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under this chapter.

(f) A processor shall not process or transfer personal data on the behalf of a controller if the processor has actual knowledge that the controller has violated this chapter with respect to such personal data.

Section 8. Data Protection Assessments.

(a) A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment for each of the controller's processing activities that presents such heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:

(1) The collection or processing of personal data for the purposes of targeted advertising;

(2) the sale of personal data;

(3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

(i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers,

(ii) financial, physical or reputational injury to consumers,

(iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or

(iv) other substantial injury to consumers;

(4) the collection or processing of sensitive data; and

(5) the collection or processing of personal information collected via a consumer's use of a product or service predominantly used by minors.

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify the categories of personal data collected, the purposes for collecting such personal data, whether personal data is being transferred and identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that are employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) No later than 30 days after completing a data protection assessment under this section, a controller shall submit a report of the data protection assessment or evaluation to the attorney general. The report must include a summary of the data protection assessment and the controller shall make the summary publicly available in a place that is easily accessible to consumers. Controllers may redact trade secrets or other confidential or proprietary information from the report. The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available to the attorney general. The attorney general may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter. To the extent any information contained in a data protection assessment disclosed to the attorney general includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

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

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

(f) A controller shall review and update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of personal data collected or processed

and level of risk presented by the processing, throughout the processing activity's lifecycle in order to:

(1) monitor for harm caused by the processing and adjust safeguards accordingly; and

(2) ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing.

Section 9. De-identified data.

(a) Any controller in possession of de-identified data shall:

(1) Take technical measures to ensure that the data cannot be associated with an individual;

(2) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

(3) contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

(b) Nothing in this chapter shall be construed to:

(1) Require a controller or processor to re-identify de-identified data; or

(2) maintain data in identifiable form, or collect, obtain, retain or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(c) Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

(1) is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data; and

(2) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer;

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

Section 10. Limitations.

(a) Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

(1) Comply with federal, state or municipal ordinances or regulations;

(2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities, except as prohibited by another law, including, but not limited to, section 115 of chapter 93;

(3) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations;

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

(5) provide, maintain, improve, or update a product or service specifically requested by the consumer;

(6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(7) take steps at the request of a consumer prior to entering into a contract;

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

(9) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity targeted at or involving the controller or processor or its services, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action, provided that for the purposes of this paragraph, "illegal activity" means a violation of a federal, state, or local law punishable as a felony or misdemeanor that can directly harm;

(10) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all relevant laws and regulations governing such research, if applicable, and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine,

(i) whether the deletion of personal data requested by a consumer under section 4, subsection (a), paragraph (4) is likely to provide substantial benefits that do not exclusively accrue to the controller,

(ii) the expected benefits of the research outweigh the privacy risks, and

(iii) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

(11) assist another controller, processor or third party with any of the obligations under this chapter;

(12) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is

(i) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and

(ii) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law;

(13) ensure the data security and integrity of personal data as required by this chapter, protect against spam, or protect and maintain networks and systems, including through diagnostics, debugging, and repairs;

(14) effectuate a product recall pursuant to federal or state law, or to fulfill a warranty;

(15) conduct medical research in compliance with part 46 of title 45, Code of Federal Regulations, or parts 50 and 56 of title 21, Code of Federal Regulations

(16) publish 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;

(17) process personal data previously collected in accordance with this chapter such that the personal data becomes de-identified data, including to:

(i) Conduct internal research to develop, improve or repair products, services or technology;

(ii) identify and repair technical errors that impair existing or intended functionality; or;

(iii) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party; or

(18) provide information or feedback to the consumer either in response to a query or for the purpose of providing a product or service requested by the consumer.

(b) The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this state. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

(c) A controller or processor that discloses personal data to a processor or third-party controller in accordance with this chapter shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes such personal data violates said sections, provided, at the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller would violate said sections. A third-party controller or processor receiving personal data from a controller or processor in compliance with this chapter is likewise not in violation of said sections for the transgressions of the controller or processor from which such third-party controller or processor receives such personal data.

(d) Nothing in this chapter shall be construed to:

(1) Impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution or Article 16 of the Massachusetts Declaration of Rights;

(2) apply to any person's collection or processing of personal data in the course of such person's purely personal or household activities; or

(3) for private schools approved under section 1 of chapter 76 and private institutions of higher education as defined by title I of the Higher Education Act of 1965, 20 United States Code, Section 1001 et seq., require deletion of personal data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.

(e) Personal data collected or processed by a controller pursuant to this section may be collected or processed to the extent that such collection and processing is:

(1) Reasonably necessary and proportionate to the purposes listed in this section, or, in the case of sensitive data, strictly necessary to the purposes listed in this section;

(2) limited to what is necessary in relation to the specific purposes listed in this section. Personal data processed pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of such processing. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such processing of personal data; and

(3) compliant with subsection (f) of section 4.

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

Section 11. Rulemaking.

(a) The attorney general may promulgate rules and regulations to implement this Act, including, but not limited to, rules and regulations that:

(1) establish or adopt baseline technical requirements that determine if a given dataset has been or can be considered sufficiently de-identified;

(2) establish reasonable administrative, technical and physical data security practices that satisfy the requirements set forward in paragraph (5) of subsection (a) of section 6;

(3) establish a nonexclusive list of practices that constitute dark patterns or otherwise violate the requirements of this chapter regarding a consumer’s affirmative consent; and

(4) establish a nonexclusive list of data collection, processing, and transfer practices that constitute unfair or deceptive practices in trade or commerce.

Section 12. Enforcement.

(a) A violation of this chapter shall constitute an unfair or deceptive trade practice for purposes of chapter 93A. Notwithstanding sections 9 and 11 of said chapter 93A, the attorney general shall have exclusive authority to bring a civil action against any controller or processor other than a controller or processor that is a large data holder that violates this chapter or a regulation adopted under this chapter to:

(1) enjoin an act or practice that is in violation of this chapter or a regulation adopted under this chapter, including an order that an entity retrieve any personal data transferred in such violation;

(2) enforce compliance with this chapter or a regulation adopted under this chapter, including seeking declaratory relief;

(3) obtain damages, including punitive damages, restitution of any money or property obtained directly or indirectly by any such violation, and disgorgement of any profits, assets, property, or data obtained directly or indirectly by any such violation on behalf of the residents of the commonwealth;

(4) impose civil penalties in an amount not more than $5,000 per violation;

(5) obtain investigative costs, reasonable attorney’s fees and other litigation costs, including, but not limited to, expert fees, reasonably incurred; and

(6) obtain any such other and further relief as the court may deem proper.

(b) If the court finds that a defendant has engaged in flagrant, willful, and repeated violations of this chapter in an action brought by the attorney general pursuant to subsection (a) of this section, the court may issue an order to suspend or prohibit the defendant from operating in the commonwealth in addition to any other remedies under subsection (a) of this section.

(c) When calculating awards and civil penalties in any action under this section, the court shall consider:

(1) the number of affected individuals and the amount and sensitivity of any personal data at issue;

(2) the severity of the violation or noncompliance;

(3) the risks caused by the violation or noncompliance;

(4) whether the violation or noncompliance was part of a pattern of noncompliance and violations and not an isolated instance;

(5) whether the violation or noncompliance was willful and not the result of error;

(6) the precautions taken by the defendant to prevent a violation;

(7) the number of administrative actions, lawsuits, settlements, and consent-decrees under this chapter involving the defendant;

(8) the number of administrative actions, lawsuits, settlements, and consent-decrees involving the defendant in other states and at the federal level in issues involving information privacy; and

(9) the international record of the defendant when it comes to information privacy issues.

(d) Any provision of a contract or agreement of any kind, including but not limited to a controller's terms of service or a privacy policy that purports to waive or limit in any way an individual's rights under this chapter, including but not limited to any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable.

(e) The attorney general shall create, maintain and monitor a mechanism for consumers to report potential violations of this chapter.

(f) The attorney general shall issue an annual report to the clerks of the house and senate, the speaker of the house, the senate president, and the house and senate chairs of the joint committee on advanced information technology, the Internet and cybersecurity in a manner consistent with the requirements of section 11 of chapter 12, provided, however, that such report shall only relate to the enforcement of this chapter and its regulations.

Section 13. Relationship to Other Laws

Nothing in this chapter shall diminish any individual's rights or obligations under any other chapter or under any regulations promulgated thereunder.

Section 14. Location Information of Non-Residents

(a) With respect to precise geolocation data that reveals that an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals is presently or was previously in the Commonwealth of Massachusetts:

(1) an individual shall have the same rights, privileges, and protections as a consumer under this chapter for all such precise geolocation data; and

(2) a controller shall treat such precise geolocation data in the same manner as it would the precise geolocation data of a consumer under this chapter.

(b) Subsection (a) does not apply to the extent that an individual is acting as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency, but only if the individual's precise geolocation data is collected, processed, or transferred solely in relation to that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

Section 15. Mergers, Acquisitions, and Bankruptcies

(a) A controller may transfer personal data to a third party in the context of a merger, acquisition, bankruptcy or similar transaction when the third party assumes control, in whole or in part, of the controller's assets, only if the controller, in a reasonable time prior to the transfer, provides an affected consumer with:

(1) notice describing the transfer, including the name of the entity receiving the consumer's personal data and the applicable privacy policies of such entity; and

(2) a reasonable opportunity to withdraw previously provided consent related to the consumer's personal data or otherwise exercise the rights guaranteed by this chapter.

(b) In any transaction involving the transfer of genetic, neural, or biometric data, the reasonable opportunity under paragraph (2) of subsection (a) shall be no shorter than 60 days.

(c) Nothing in this section shall be construed to diminish the requirements of paragraph (6) of subsection (a) of section 6.

Section 16. Browser Privacy Settings

By January 1, 2027, a person shall not develop or maintain a browser that does not include a setting that enables a consumer to send an opt-out preference signal, as described in section 6(e)(2), to controllers or processors that the consumer interacts with through the browser.

SECTION 2. SECTION 1 shall take effect 180 days after enactment.

SECTION 3. The first data protection assessments required by section 8 of the Massachusetts Consumer Data Privacy Act shall be completed no later than the first anniversary of the effective date of this Act.