HOUSE . . . . . No. 5472

The Commonwealth of Massachusetts

HOUSE OF REPRESENTATIVES, June 3, 2026.

The committee on Ways and Means, to whom was referred the Senate Bill establishing the Massachusetts data privacy act (Senate, No. 2619) reports recommending that the same ought to pass with amendments striking out all after the enacting clause and inserting in place thereof the text contained in House document numbered 5472; by striking out the title and inserting in place thereof the following title: "An Act establishing the Massachusetts consumer data privacy act.".

For the committee,

AARON MICHLEWITZ.

HOUSE . . . . . No. 5472

The Commonwealth of Massachusetts

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

By striking out all after the enacting clause and inserting in place thereof the following:–

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

Chapter 93M

Consumer Data Privacy

Section 1. As used in this chapter, the following words shall, unless the context clearly requires otherwise, have the following meanings:

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

(i) ownership of, or the power to vote, more than 50 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", a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement, including authorization for an act or practice; provided, that "affirmative consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action; and provided further, that "affirmative consent" shall not include: (i) acceptance of general or broad terms of use or a 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", 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", data generated by automatic measurements of an individual's biological characteristics, including: (i) a fingerprint; (ii) a voiceprint; (iii) eye retinas; (iv) irises; (v) gait; or (vi) other unique biological patterns or characteristics that can be used to identify a specific individual; provided, however, that "biometric data" shall not include: (A) a digital or physical photograph; (B) an audio or video recording; or (C) 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.

"Business associate", as defined in the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.

"Child", as defined in the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq.

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

"Consumer", an individual who is a resident of the commonwealth; provided, however, that "consumer" shall not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, corporation, partnership, sole proprietorship, nonprofit organization or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, corporation, partnership, sole proprietorship, nonprofit organization or government agency.

"Consumer health and wellness data", personal data that is collected in real time or retroactively by a health and wellness device or application, which is designed to allow a consumer to track or monitor information regarding the consumer's health and wellness, including, but not limited to: (i) fitness; (ii) nutrition; (iii) diet; (iv) physical activity; (v) sleep; (vi) mental state; (vii) stress; or (viii) behavior. "Consumer health and wellness data" shall not include biometric data, neural data, genetic data or personal data that reveals a mental or physical health condition, diagnosis, disability or treatment.

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

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

"Covered entity", as defined in the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.

"Dark pattern", a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice; provided, that "dark pattern" shall include, but shall not be 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", any decision made by the controller, or on behalf of the controller, that result in the provision of, or denial by, the controller of any: (i) financial or lending services; (ii) housing; (iii) insurance; (iv) education enrollment or opportunity; (v) criminal justice; (vi) employment opportunities; (vii) health care services; or (viii) access to essential goods or services.

"De-identified data", 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 clauses (i) and (ii).

"Gender-affirming health care services", as defined in section 11I½ of chapter 12.

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

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

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

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

"Large data holder", a controller or processor that in the most recent calendar year collected, processed or sold the: (i) personal data of more than 2,000,000 consumers; provided, however, that said personal data shall not include personal 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 (ii) sensitive data of more than 200,000 consumers.

"Legally-protected health care activity", as defined in section 11I½ of chapter 12.

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

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

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

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

"Personal data", any information, including derived data, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual; provided, however, that "personal data" shall not include de-identified data or publicly available information.

"Precise geolocation data", 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 specific 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" shall 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", any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, including, but not limited to, the: (i) use; (ii) storage; (iii) disclosure; (iv) analysis; and (v) deletion or modification of personal data.

"Processor", a person who collects or processes personal data on behalf of, or at the direction of: (i) a controller; (ii) another processor; or (iii) a federal, state, tribal or local government entity.

"Profiling", any form of processing performed on personal data to evaluate, analyze or predict personal aspects, including, but not limited to, an individual's: (i) economic situation; (ii) health; (iii) personal preferences; (iv) interests; (v) reliability; (vi) behavior; (vii) location; or (viii) movements.

"Protected health information", as defined in the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.

"Publicly available information", information that is lawfully made available to the general public from: (i) federal, state or municipal government records; (ii) widely distributed media; or (iii) a disclosure to the general public as required by federal, state or local law; provided, that a controller shall have a reasonable basis to believe that: (A) a consumer has lawfully made the information available to the general public; or (B) the information has been lawfully made available to the general public from widely distributed media. "Publicly available information" shall not include: (i) any obscene visual depiction, as defined in 18 U.S.C. 1460; (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) genetic or neural data, unless otherwise made publicly available by the individual to whom the information pertains; (v) 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 (vi) 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", 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 11I½ 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", 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", the exchange, disclosure, release, dissemination, license or rental of personal data, or other means of making personal data available, for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" shall 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 sale 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;

(v) the disclosure or sale 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 or sale of personal data to a third party as part of a merger, acquisition, bankruptcy or similar transaction where the third party assumes control, in whole or in part, of the controller's assets; provided, that the controller shall, in a reasonable time prior to the disclosure or transfer, provide an affected consumer with: (i) notice describing the transfer,

including, but not limited to: (A) the name of the entity receiving the consumer's personal data; and (B) the applicable privacy policies of such entity; and (ii) a reasonable opportunity to withdraw affirmative consent related to the consumer's personal data or otherwise exercise the rights guaranteed by this chapter; provided, that said reasonable opportunity shall be not less than 60 days if the sale is related to genetic data, neural data or biometric data; provided further, that nothing shall be construed to change the requirements of paragraph (3) of section 6.

"Sensitive data", 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 data

(iv) neural data;

(v) biometric data;

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

(vii) precise geolocation data;

(viii) 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

(ix) account names, passwords, usernames that are not publicly available or that have a restricted audience, access codes, security questions or answers or other credentials and information used to log in to an account or device, including, but not limited to, passkeys.

"Targeted advertising", displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated internet web sites or online applications to predict such consumer's preferences or interests; provided, however, that "targeted advertising" shall not include:

(i) advertisements based on activities within a controller's own websites or online applications;

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

(iii) advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(iv) processing personal data solely to measure or report advertising frequency, performance or reach.

"Third party", 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" shall not include a person that collects personal data from another entity if the 2 entities are affiliates.

"Trade secret", as defined in section 42 of chapter 93.

Section 2. This chapter shall apply to persons that conduct business in the commonwealth and produce products or provide services that are targeted to residents of the commonwealth and that, during the preceding calendar year:

(i) collected or processed the personal data of not less than 100,000 consumers; provided, however, that said personal data shall not include personal data controlled or processed solely for the purpose of completing a payment transaction;

(ii) derived gross revenue of not less than $100,000 from the sale of personal data; or

(iii) collected or processed sensitive data; provided, however, that sensitive data shall not include personal data controlled or processed solely for the purpose of completing a payment transaction.

Section 3. (a) This chapter shall 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 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 U.S.C. 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;

(6) an educational nonprofit organization, including an institution of higher education;

(7) a nonprofit organization that establishes or maintains a blood bank or transfusion service pursuant to section 184B of chapter 111 and in compliance with applicable requirements of the U.S. Food and Drug Administration, including, but not limited to, 21 C.F.R. parts 600, 601, 606, 607, 610, 630 and 640, as amended, and any successor provisions; or

(8) 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) Notwithstanding subsection (a), any entity exempt pursuant to subsection (a) shall comply with clause (i) of subsection (a) of section 7.

(c) The following information and data shall be exempt from 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 chapter;

(2) patient-identifying information for purposes of 42 U.S.C. 290dd-2;

(3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. 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 Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(5) the protection of human subjects under 21 C.F.R. parts 50 and 56, or personal data used or shared in research, as defined in 45 C.F.R. 164.501, that is conducted in accordance with the standards set forth in this paragraph and paragraphs (3) and (4), 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 U.S.C. 11101 et seq.;

(7) patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. 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 U.S.C. 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 U.S.C. 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 U.S.C. 2721 et seq., as amended from time to time;

(12) personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. 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 U.S.C. 2001 et seq., as amended from time to time;

(14) data collected or processed: (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) 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 U.S.C. 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 U.S.C. 41713, as said acts may be amended from time to time.

(d) 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. (a) A consumer shall have the right to:

(1) confirm whether 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; provided, however, that such confirmation or access shall not require the controller to reveal a trade secret;

(2) obtain from a controller a list of third parties, other than natural persons, to which the controller has sold either: (i) the consumer's personal data; or (ii) any personal data; provided, however, that such confirmation or access shall not require the controller to reveal a trade secret;

(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;

(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;

(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 pursuant to section 8. A consumer may designate an authorized agent in accordance with section 5 to exercise the rights of such consumer specified in this section on behalf of the consumer.

(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 this section 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 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests; provided, that the controller shall inform the consumer of any such extension and the reason for the extension within the initial 45-day response period.

(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 12-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 shall bear the burden of demonstrating that a request is manifestly unfounded, excessive or repetitive.

(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) 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 until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right; provided, that any such information shall not be used for any purpose other than the authentication of the 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 the 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 the controller believes the request is fraudulent, why such controller believes the request is fraudulent and that the controller shall not comply with the 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 personal data pursuant to paragraph (4) of subsection (a) 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 subsection (b). 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 decision. If the appeal is denied, the controller shall provide the consumer with an online mechanism, if available, or other method, including mail or in person, through which the consumer may contact the attorney general to submit a complaint.

(e) A controller shall not condition, effectively condition, attempt to condition or attempt to effectively condition the exercise of a right described in this section through the use of: (i) any false, fictitious, fraudulent or materially misleading statement or representation; or (ii) dark patterns.

(f) A controller or processor shall not collect or process personal data in a manner that unlawfully discriminates against an individual or class of individuals, threatens to discriminate 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, national origin, citizenship or immigration status or any other basis protected by chapter 151B.

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

(i) the collection or processing of personal data for the sole purpose of: (A) a controller or processor's self-testing to prevent or mitigate unlawful discrimination or otherwise to ensure compliance with state or federal law; or (B) diversifying an applicant, participant or customer pool; or

(ii) a private establishment, as described in 42 U.S.C. 2000a(e).

Section 5. (a) A consumer may designate another person to serve as the consumer's authorized agent to act on such consumer's behalf to exercise rights specified in paragraph (6) of subsection (a) of section 4. A parent or legal guardian of a minor may exercise a consumer right under said subsection (a) of said section 4 on the minor's behalf. For a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or conservator of the consumer may exercise a consumer right under said subsection (a) of said section 4 on the consumer's behalf.

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

Section 6. A controller shall:

(1) limit the collection of personal data to what is reasonably necessary and proportionate in relation to the purposes for which the personal data is collected or processed, as disclosed to

the consumer; provided, that in determining what is reasonably necessary and proportionate the following shall be taken into account, the: (i) consumer's reasonable expectation regarding the personal data at the time the personal data was collected based on the purposes that were disclosed to the consumer; (ii) relationship that the new purpose bears to the purposes that were disclosed to the consumer; (iii) impact that processing the personal data for the new purpose might have on the consumer; (iv) relationship between the consumer and the controller and the context in which the personal data were collected; and (v) existence of additional safeguards, including, but not limited to, encryption, in processing such personal data for such new purpose;

(2) unless the controller obtains the consumer's affirmative consent, not process the consumer's personal data for any materially new purpose that is neither reasonably necessary to, nor compatible with, the purposes that were disclosed to the consumer;

(3) not collect or process sensitive data concerning a consumer without obtaining the consumer's affirmative consent, or, in the case of the processing of sensitive data concerning a known child, without processing such sensitive data in accordance with COPPA;

(4) 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, but not limited to, disposing of personal data in accordance with a retention schedule that requires the deletion of personal data when the personal data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected or processed; and

(5) provide an effective mechanism for a consumer to revoke the consumer's affirmative consent 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 personal data as soon as practicable, but not later than 15 days after the receipt of such request.

Section 7. (a) A controller shall not:

(i) sell: (A) precise geolocation data of any individual or consumer collected or processed within the commonwealth, regardless of the residency of the individual or consumer; provided, that precise geolocation data shall not be sold even with the affirmative consent of an individual or consumer; or (B) sensitive data other than precise geolocation data without obtaining the consumer's affirmative consent; and provided further, that in the case of the collection or processing of personal data concerning a known child, personal data shall be collected and processed in accordance with COPPA;

(ii) collect or process the personal data of a consumer for purposes of targeted 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; or

(iii) discriminate or retaliate against a consumer, or threaten to 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 specific product or service, including, but not limited to, 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)(1) Nothing in paragraph (iii) of subsection (a) shall be construed to require a controller to provide a specific 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: (i) the controller shall not sell personal data to a third party as part of such program unless such sale is clearly and conspicuously disclosed in the terms of the program; and (ii) the sale of personal data shall not be a condition of participation in the program.

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

Section 8. (a) A controller shall provide consumers with a reasonably accessible, clear and not misleading privacy notice that shall include:

(i) 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 with an understanding of the type of personal data collected or processed;

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

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

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

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

(vi) 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

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

(b)(1) The privacy notice shall be provided directly to consumers and made publicly available online. 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 shall provide a reasonable opportunity for each consumer to withdraw affirmative consent. 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.

(2) A controller shall provide a reasonable opportunity for each consumer to affirmatively consent to further materially different processing or sale of previously collected personal data under the changed notice.

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

(d)(1) A controller shall establish, and shall describe in a privacy notice, not less than 2 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 authenticate the identity of the consumer making the request. A controller shall not require a consumer to create a new account to exercise consumer rights but may require a consumer to use an existing account.

(2) Any means for a consumer to exercise their consumer rights established pursuant to paragraph (1) shall include 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 the commonwealth 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.

(3) 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 this subsection conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's financial incentive program, including a bona fide loyalty, rewards, premium features, discounts, club card or

similar 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.

Section 9. (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. A processor's 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 reasonable, 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; and

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

(b)(1) 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: (i) instructions for processing data; (ii) the nature and purpose of processing; (iii) the type of data subject to processing; (iv) the duration of processing; and (v) 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 shall only process 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.

(2) The contract between a controller and a processor shall require that the processor:

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

(ii) 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;

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

(iv) 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;

(v) 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 unless directed to do so by the controller; and

(vi) 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; provided, that the processor shall provide a report of such assessment to the controller upon request.

(3) Nothing in the contract pursuant to paragraphs (1) and (2) 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.

(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 appropriate to the volume and nature of the personal data at issue.

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of personal data shall be 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, shall be considered a controller and not a processor with respect to a specific processing of personal data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data shall remain a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor shall be considered a controller with respect to such processing and may be subject to an enforcement action under this chapter.

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

Section 10. (a) For the purposes of this section, the words "processing activities that presents a heightened risk of harm to a consumer" shall include:

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

(2) the sale of personal data;

(3) processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of: (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (B) financial, physical or reputational injury to consumers; (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (D) other substantial injury to consumers;

(4) processing of sensitive data; and

(5) processing of personal data where such personal data was processed through a consumer's use of a product or service predominantly used by minors.

(b) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer.

(c) Data protection assessments shall identify: (i) the categories of personal data processed; (ii) the purposes for processing such personal data; (iii) whether personal data is being sold; and (iv) 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.

(d) The attorney general may require a controller to 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 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.

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

(f) 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 under this section.

(g) A controller shall review and update the data protection assessment as often as appropriate.

Section 11. (a) Any controller who has collected or processed personal data and is in possession of de-identified data shall:

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

(2) publicly commit to maintaining and using de-identified data without attempting to re-identify the personal 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 require a controller or processor to:

(1) re-identify de-identified data;

(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; or

(3) comply with an authenticated consumer rights request if the controller: (A) 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 (B) 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.

(c) A controller that sells 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 12. (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;

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

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

(12) 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;

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

(14) conduct medical research in compliance with 45 C.F.R. part 46 or 21 C.F.R. parts 50 and 56;

(15) publish entity-based member or employee contact information where such publication is intended to allow members of the public to contact such entity-based member or employee in the ordinary course of the entity's operations;

(16) process personal data previously collected in accordance with this chapter such that the personal data becomes de-identified data, including to: (A) conduct internal research to develop, improve or repair products, services or technology; (B) identify and repair technical

errors that impair existing or intended functionality; or (C) 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;

(17) 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; or

(18) with the consent of the consumer, collect or process the consumer's biometric data using facial recognition technology for the purposes of permitting entry to a ticketed event in a location closed to the public; provided, that the biometric data shall not be used for any other purpose and shall be de-identified as soon as practicable; and provided further, that no biometric data shall be sold to any third party.

(b) The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under the laws of the commonwealth. 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 commonwealth as part of a privileged communication.

(c)(1) 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 this chapter if the processor or third party controller that receives and processes such personal data violates this chapter; provided, that at the time the 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 this chapter.

(2) A third party controller or processor receiving personal data from a controller or processor in compliance with this chapter shall not be in violation of this chapter 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: (i) 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 XVI of the Declaration of Rights; or (ii) apply to any person's collection or processing of personal data in the course of such person's purely personal or household activities.

(e) Personal data collected or processed by a controller under this section may be collected or processed to the extent that such collection and processing is consistent with this chapter.

Section 13. (a) The attorney general shall promulgate rules or regulations to implement this chapter, including, but not limited to, rules and regulations that establish:

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

(ii) reasonable administrative, technical and physical data security practices that satisfy the requirements set forward in paragraph (4) of section 6;

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

(iv) a nonexclusive list of data collection or processing practices that constitute unfair or deceptive practices in trade or commerce;

(v) the frequency for which the controller shall review and update the data protection assessment under section 10; and

(vi) requirements for privacy notices under section 8.

Section 14. (a)(1) A violation of this chapter shall constitute an unfair or deceptive trade practice for purposes of chapter 93A.

(2) Notwithstanding sections 9 and 11 of chapter 93A, the attorney general shall have exclusive authority to bring a civil action against any controller or processor other than a large data holder that violates this chapter or a regulation adopted under this chapter to:

(i) 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;

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

(iii) 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 personal data obtained directly or indirectly by any violation on behalf of the residents of the commonwealth;

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

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

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

(3) The restitution recovery for any violation of this chapter awarded as the result of a class action shall be reduced by any restitution amounts recovered by the attorney general for the same violation. Determination of damages shall be stayed until the attorney general notifies the court of any such recovery or that it is not seeking recovery in the matter, but in no event more than 1 year after a finding of liability or the filing of a stipulated judgement.

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

(c) Annually, not later than March 1, the attorney general shall issue a report to the clerks of the house of representatives and senate and the chairs of the joint committee on advanced information technology, the internet and cybersecurity in a manner consistent with section 11 of chapter 12 on any enforcement actions taken pursuant to this section and the status or outcomes of said enforcement actions; provided, however, that such report shall relate to the enforcement of this chapter and its regulations; and provided further, that the attorney general may incorporate the report required pursuant to this subsection in the annual report pursuant to said section 11 of said chapter 12.

SECTION 2. The data protection assessments required by section 10 of chapter 93M of the General Laws, inserted by section 1, shall not be requested by the attorney general before July 1, 2028.

SECTION 3. Not later than May 1, 2027, the attorney general shall promulgate rules or regulations required pursuant to section 13 of chapter 93M of the General Laws, inserted by section 1.

SECTION 4. The first report required pursuant to section 14 of chapter 93M of the General Laws, inserted by section 1, shall be submitted not later than March 1, 2028.

SECTION 5. Section 1 shall take effect July 1, 2027.; and by striking out the title and inserting in place thereof the following title: “An Act establishing the Massachusetts consumer data privacy act.”.