**Bill Number: H. 104**
**Title:** An Act establishing the Massachusetts Data Privacy Act
**Lead Sponsor:** Representative Andres Vargas, Representative David Rogers
**Hearing Date:** April 9, 2025
**Report Date:** June 8, 2025
**See Senate Filing:** S. 45

**Current Law:**

- **M.G.L. Chapter 66A** regulates government uses and protection of personal information.
- **M.G.L. Chapter 90 § 1** defines "device," in part, as used in the bill.
- **M.G.L. Chapter 93A** prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce.
- **M.G.L. Chapter 93A § 4** outlines how the Attorney General may bring suit for a violation of Chapter 93A.
- **M.G.L. Chapter 93A § 9** outlines how a consumer or class may bring suit for a violation of Chapter 93A
- **M.G.L. Chapter 93H** outlines the requirements for notification for data breaches.
- **M.G.L. Chapter 151B** prohibits employment discrimination based on status as a member of a protected class.
- **M.G.L. Chapter 214 § 1B** establishes an equitable right of privacy that may be enforced by the superior court.
- **M.G.L. Chapter 214 § 3B** establishes liability for violations of Chapter 66A.

**Executive Summary:** Establishes baseline data minimization standards by restricting data holders to only collect and process what is reasonably necessary and proportional to their lawful purpose. The MDPA will ensure greater accountability of companies and grant user data privacy protections to those present in Massachusetts and residents of the state. Highlighted in this bill are strong protections for children, defined as anyone under 18 years, from targeted advertising and transferring of their data without expressed consent. The Attorney General is empowered with rulemaking authority and to enforce violations under the Commonwealth's consumer protection law, Chapter 93A. Consumers are also able to bring claims on their own behalf through a private right of action.

**Legislative History:** New File; Reported out of AITIC Committee favorably May 2024 as H.4631

***SECTION 1: Comprehensive Privacy***
The General Laws, as appearing in the 2022 Official Edition, are hereby amended by inserting after chapter 93K the following chapter:
Chapter 93M. Massachusetts Data Privacy Act
Coverage: Data subject rights extend to all individuals located in Massachusetts.

***Section 1. Definitions***

Key Definitions Include:

Covered entities include any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data. Does not include government entities, entities that made less than $20,000,000 over 3 years, processed or collected data of less than 25,000 individuals. An entity that derives any revenue from transferring covered data is a covered entity.

Consent is defined as a clear affirmative act signifying an individual's freely given, specific, informed, and unambiguous agreement to allow the processing of specific categories of personal information. Consent does not include hovering over, muting, pausing, or closing a given piece of content (e.g. clicking out of a prompt is not consent.)

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

***Section 2. Duty of Loyalty***

Establishes baseline data minimization standards by restricting data holders to only collect and process what is reasonably necessary and proportional to their lawful purpose. Clarifies lawful bases for processing personal information.

Prohibits the use of any dark patterns or deceptive designs that may trick consumers into agreeing to policies against their best interests.

***Section 3. Sensitive Covered Data***

Establishes more restrictive standards for the purposes of processing sensitive data such as precise geolocation information, biometric or genetic information, the covered data of a minor (anyone under 18), government-issued identifiers and covered data that reveals an individual's:

- race, color, ethnicity, or national origin
- sex or gender identity
- religious beliefs
- citizenship or immigration status
- military service
- status as a victim of a crime
- sexual orientation

Sensitive data includes the type of information that a person would have a reasonable expectation of privacy over. This encompasses data that may reveal an individual's private communications such as voicemails, emails, texts, direct messages, or an individual's calendar information, address book information, phone or text logs, or covered data that reveals an individual's online activities over time and across third-party websites or online services.

Sensitive data cannot be processed for the purposes of targeted advertising. Covered entities cannot transfer an individual's sensitive covered data to a third party without the affirmative express consent of the individual (given before each specific transfer).

***Section 4. Data Subject Rights***

Empowers consumers to have the right to be informed about a covered entity's data practices. These core data-subject rights included in the legislation are the most common across data privacy laws across the country and around the world.

- Right to Access
    - Individuals may request (in a human-readable format) their personal information that was collected, processed, or transferred by the covered entity within the 12 months preceding the request.
    - If the covered entity transfers this data to any third parties, then the consumer is also able to request the categories of any third party or service provider and an option for consumers to obtain the names of any such third party.
    - The consumer may also request the categories of sources from which the covered data was collected and a description of the purpose for which the covered entity transferred the covered data.
- Right to Correct
    - Individuals may request to correct any verifiable substantial inaccuracy or substantially incomplete information that is processed by the covered entity.
    - Individuals may instruct the covered entity to notify all third parties or service providers to which the covered entity has transferred this covered data about the corrected information.
- Right to Delete
    - Individuals may request to delete their covered data that is processed by the covered entity.
    - Individuals may instruct the covered entity to notify all third parties of the individual's deletion request.
    - A covered entity may decline, with adequate explanation to the individual, to comply with a request for deletion if the request:
        - unreasonably interferes with the provision of products or services by the covered entity to another person it currently serves
        - requests to delete covered data that relates to a public figure or public official
        - requests to delete covered data that the covered entity reasonably believes may be evidence of unlawful activity
    - Includes a provision that consumers cannot request to delete covered data that is used to evaluate a consumer's creditworthiness, credit standing, credit capacity (i.e. consumers cannot request to delete their credit reports)
- Right to Transport
    - Individuals may request an export (to themselves or directly to another entity) of their covered data that is processed, including inferences linked or reasonably linkable to the individual.

Covered entities must comply with legitimate consumer requests to exercise these rights. Covered entities must also include a mechanism for consumers to exercise these rights in the same location as their privacy notice. Covered entities may deny requests under specific circumstances, and with reasonable explanation to the individual who made the request.

*Section 5. Consent Practices*
Outlines acceptable consent practices between covered entities and consumers (clear and conspicuous requests for consent to collect and process information, reasonably understandable language, etc.)
The request for consent must include a reasonably understandable description of the processing purpose, clearly state the specific categories of covered data that the covered entity shall collect, process, and transfer. The request must clearly explain an individual's applicable rights. The request for consent must be displayed at or before the point of collection of information. The consent request must be accompanied with a copy of the covered entity's Privacy Policy (subject to the requirements of Section 9).
Covered entities cannot infer that an individual has provided consent via their inaction or the individual's continued use of a service or product. (e.g. clicking out of the consent request without confirming collection choices does not equate consent.)

***Section 6. Privacy by Design***
Requires covered entities to establish, implement, and maintain reasonable policies, practices, and other procedures that reflect their role in collecting, processing, and transferring covered data. Such policies and practices should:

- Consider applicable federal and state laws or regulations related to covered data the entity collects, processes, or transfers.
- Identify, assess, and mitigate privacy risks related to minors.
- Mitigate privacy risks as a whole.
- Evaluate the length of time data shall be retained and the sensitivity of the data (e.g. delete, de-identify or otherwise modify data when it is no longer needed).
- Implement reasonable training and safeguards to promote compliance with all privacy laws applicable to covered data the covered entity collects, processes, or transfers.

***Section 7. Pricing***
Covered entities cannot alter prices or limit services to an individual in retaliation if that individual has chosen to exercise their data subject rights (as outlined in Section 4) or withheld consent to certain collection or processing.

***Section 8. Civil Rights Protections***
A covered entity may not collect, process, or transfer covered data or publicly available data in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services in accordance with pre-existing anti-discrimination laws in Massachusetts.
Requires that whenever the Attorney General obtains information that a covered entity or service provider may have collected, processed, or transferred covered data in violation of this

section, the Attorney General shall initiate enforcement actions relating to such violation in accordance with Section 12 of this chapter.
Requires that the Attorney General submit an annual report to the Joint Committee on Ways and Means, the Joint committee on Racial Equity, Civil Rights, and Inclusion, and the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity on enforcement actions taken under this subsection.

***Section 9. Privacy Policy***

Requires that each covered entity make publicly available, in a clear and conspicuous location on its homepage, a reasonably understandable and not misleading privacy policy that provides a detailed and accurate representation of the data collection, processing, and transfer activities of the covered entity or service provider.
The privacy policy must include information such as the contact information for privacy and data security inquiries, the categories of covered data the covered entity collects or processes and the processing purposes for each category, data retention practices and information on whether the covered entity transfers covered data.

- If the covered entity transfers data the privacy policy must list each category of service provider and third party, the name of each data broker to which the covered entity or service provider transfers covered data, and the purposes for which such data is transferred.
- Requires that if a covered entity makes a material change to its privacy policy or practices, the covered entity must notify each individual affected before implementing the change to provide a reasonable opportunity for each individual to withdraw consent.

The privacy policy must also include a prominent, clear, and reasonably understandable description of how an individual can exercise their rights as described in this chapter.
Requires that each covered entity that collects, processes, or transfers biometric data or precise geolocation information to provide an additional separate privacy policy detailing the collection, processing, and transfer of such data.

- Requires that a large data holder retain copies of previous versions of its privacy policy for at least 10 years beginning after the date of enactment of this chapter and publish them on its website.
- In addition to the privacy policy required, a large data holder is required to provide a short form notice of no more than 500 words in length that includes the main features of their data practices.

***Section 10. Advanced Data Rights***

Requires covered entities to provide an individual with a clear and conspicuous, easy-to-execute mechanism to withdraw consent and opt out of certain data practices. These means are required, at a minimum, to be accessible in the same location as the privacy policy outlined in Section 9. Requires that a covered entity that receives an opt out notification pursuant to this section to abide by such opt out. Such covered entity or service provider must further notify any other person that directed the entity to serve, deliver, or otherwise process targeted advertisements or to engage in profiling of the individual's opt out decision.

Requires that a covered entity notify third parties who had access to an individual's covered data when the individual exercises any of the rights established in this section. Requires that the third party comply with the request to opt out. The third party shall comply with the request in the same way a covered entity is required to comply with the request. The third party shall no longer retain, use, or disclose this personal information. A covered entity that communicates an individual's opt out request to a third party or service provider pursuant to this section shall not be liable under this chapter if the third party or service provider receiving the opt-out request violates the restrictions set forth in this chapter.

- Right to opt out of covered data transfers.
    - Requires that a covered entity may not transfer or direct the transfer of the covered data of an individual to a third party if the individual objects to the transfer.
- Right to opt out of targeted advertising. Requires that a covered entity that directly delivers a targeted advertisement must:
    - Prior to engaging in targeted advertising to an individual or device and at all times, provide the individual with a means to opt out of targeted advertising.
    - Abide by any opt out designation by an individual with respect to targeted advertising and notify the covered entity that directed the targeted advertisement of the opt out decision.
    - Allow an individual to opt out with respect to targeted advertising through an opt out mechanism, at a minimum, accessible in the same location as the privacy policies required by section 9.
- Right to opt out of profiling. Requires that a covered entity that engages in profiling in furtherance of automated decisions that produce legal or similarly significant effects on an individual shall:
    - provide such individual with a clear and conspicuous means to opt out of such profiling; and
    - allow an individual to object to such profiling through an opt out mechanism, at a minimum, accessible in the same location as the privacy policies required by section 9.

A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of any individual right under this section through:

- the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or
- the use of a dark pattern or deceptive design.

***Section 11. Service Providers***

Extends provisions to companies that solely process data on behalf of a controller (non-consumer facing). Governs the relationship between companies that collect data but contract out certain processing activities.

***Section 12. Enforcement***

A violation of this chapter constitutes an injury to that individual and shall be deemed an unfair or deceptive act or practice in the conduct of trade or commerce under Chapter 93A (The Massachusetts Consumer Protection Law).

Includes a private right of action. Any individual alleging a violation of this chapter by a covered entity that is a large data holder may bring a civil action in the superior court or any court of competent jurisdiction.

The court may award:

- Liquidated damages of not less than 0.15% of the annual global revenue of the covered entity or $15,000 per violation, whichever is greater.
- Punitive damages; and
- Any other relief, including but not limited to an injunction, that the court deems to be appropriate.

The Attorney General may bring an action pursuant to Section 4 of Chapter 93A against a covered entity, service provider, or third party to remedy violations of this chapter and for other relief, including but not limited to an injunction, that may be appropriate, subject to the following:

- If the court finds that the defendant has employed any method, act, or practice which they knew or should have known to be in violation of this chapter, the court may require the defendant to pay to the commonwealth a civil penalty of:
    - Not less than 0.15% of the annual global revenue or $15,000, whichever is greater, per violation; and
    - Not more than 4% of the annual global revenue of the covered entity, service provider, or third-party or $20,000,000, whichever is greater, per action if such action includes multiple violations to multiple individuals.
- If the court finds that a defendant has engaged in flagrant, willful and repeat violations of this chapter, the court may issue an order prohibiting or suspending a covered entity or service provider from operating in the Commonwealth, or collecting, processing, and transferring covered data and any other relief, including but not limited to an injunction, that the court deems to be appropriate.

***Section 13. Information Non-applicability***

Grants a data-level exemption for certain types of data that is already processed under federal regulations.

This chapter shall not apply to:

- Personal information captured from a patient by a health care provider or health care facility or biometric information collected, processed, used, or stored for operations under the federal Health Insurance Portability and Accountability Act of 1996.
- Nonpublic personal information that is processed by a financial institution subject to, and in compliance with, the Gramm-Leach-Bliley Act.
- Personal information regulated by the federal Family Educational Rights and Privacy Act.

- Individuals sharing their personal contact information such as email addresses with other individuals in the workplace, or other social, political, or similar settings where the purpose of the information is to facilitate communication among such individuals.
- Covered entities' publication of entity-based member or employee contact information where such publication is intended to allow members of the public to contact members or employees in the ordinary course of the entity's operations.

***Section 14. Implementation***

Requires the Attorney General to adopt rules and regulations for the implementation, administration, and enforcement of this chapter.

The rules and regulations shall include but are not limited to:

- Establishing or adopting baseline technical requirements that determine if a given dataset has been or can be considered sufficiently de-identified;
- Establishing reasonable policies, practices, and procedures that satisfy the requirements set forward in Section 6 for privacy by design.
- Establishing a nonexclusive list of practices that constitute deceptive designs or dark patterns.

Requires the Attorney General to create a website that outlines the provisions of this chapter and provides consumers with a form to report violations of this chapter. The website shall include statistics on the Attorney General's enforcement actions undertaken under this chapter.

***Section 15. Authorized Agents***

Allows an individual to designate another person to serve as the individual's authorized agent to exercise the individual's rights under this chapter. In the case of covered data concerning an individual known to be a child, the parent or legal guardian of such child may exercise the rights provided under this chapter on the child's behalf. In the case of covered data concerning an individual subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the individual may exercise the rights provided under this chapter on the individual's behalf.

***Section 16. Advertising to Minors***

A covered entity may not engage in targeted advertising to a minor.

***Section 17. Data Brokers***

Requires that data brokers shall place a clear, conspicuous, not misleading, and readily accessible notice on the website or mobile application of the data broker that:

- Notifies individuals that the entity is a data broker.
- Includes a link to the data broker registry website.
- Is reasonably accessible to and usable by individuals with disabilities.

Requires data broker registration with the OCABR, no later than January 31 of each calendar year that follows a calendar year during which a covered entity acted as a data broker.

- A data broker that fails to register or provide the notice as required under this section shall be subject to enforcement proceedings under Section 12.

Requires the OCABR to establish and maintain on a website a searchable, publicly available, central registry of third-party collecting entities that are registered with the OCABR under this subsection that includes a listing of all registered data brokers and a search feature that allows members of the public to identify individual data brokers and access to the registration information.

***SECTION 2: Location Shield Act***
The General Laws, as appearing in the 2022 Official Edition, are hereby further amended by inserting after chapter 93M the following chapter:

Chapter 93N. Privacy Protections for Location Information Derived from Electronic Devices
Coverage: Any individual, partnership, corporation, limited liability company, association, or other group, however organized. A covered entity does not include a state or local government agency, or any court of Massachusetts, a clerk of the court, or a judge or justice thereof. A covered entity does not include an individual acting in a non-commercial context. A covered entity includes all agents of the entity.

Protections apply to any person located in the Commonwealth of Massachusetts.

***Section 1. Definitions***
Key Definitions Include:
Covered entities include any individual, partnership, corporation, limited liability company, association, or other group, however organized and all agents of the entity. A covered entity does not include a state or local government agency, or any court of Massachusetts, a clerk of the court, or a judge or justice thereof. A covered entity does not include an individual acting in a non-commercial context.

Location information is information derived from a device or from interactions between devices, directly or indirectly reveals the present or past geographical location of an individual or device within Massachusetts with precision to identify street-level location information within a range of 1,850 feet or less.

***Section 2. Protection of Location Information***
It shall be unlawful for a covered entity to collect or process an individual's location information except for a permissible purpose.

Requires that prior to collecting or processing an individual's location information, a covered entity shall provide the individual with a Location Privacy Policy and obtain consent from that individual. The Location Privacy Policy, at a minimum, requires the following:

- The permissible purpose for which the covered entity is collecting, processing, or disclosing any location information.
- The type of location information collected, including the precision of the data.
- The identities of service providers with which the covered entity contracts with respect to location data.
- Any disclosures of location data necessary to carry out a permissible purpose and the identities of the third parties to whom the location information could be disclosed.
- Whether the covered entity's practices include the internal use of location information for purposes of targeted advertisement.
- The data management and data security policies governing location information.
- The retention schedule and guidelines for permanently deleting location information.

Requires that a covered entity provide notice to individuals of any change to its Location Privacy Policy at least 20 business days before the change goes into effect and shall request and obtain consent before collecting or processing location information in accordance with the new Location Privacy Policy.

Consent provided under this section shall expire:

- After one year, when the initial purpose for processing the information has been satisfied, or when the individual revokes consent, whichever occurs first.
- Upon expiration of consent, any location information possessed by a covered entity must be permanently destroyed.

Requires that a covered entity that directly delivers targeted advertisements as part of its product or services shall provide individuals with a clear, conspicuous, and simple means to opt out of the processing of their location information for purposes of selecting and delivering targeted advertisements.

Covered entities cannot:

- Collect more precise location information than necessary to carry out the permissible purpose;
- Retain location information longer than necessary to carry out the permissible purpose;
- Sell, rent, trade, or lease location information to third parties; or derive or infer from location information any data that is not necessary to carry out a permissible purpose.
- Disclose, cause to disclose, or assist with or facilitate the disclosure of an individual's location information to third parties, unless such disclosure is necessary to carry out the permissible purpose for which the information was collected, or requested by the individual to whom the location data pertains.
- Disclose location information to any federal, state, or local government agency or official unless (1) the agency or official serves a valid warrant or establishes the existence of exigent circumstances (2) disclosure is mandated under federal or state law, including in response to a court order or lawfully issued and properly served subpoena or civil investigative demand under state or federal law, or (3) the data subject requests such disclosure.

Government entities cannot monetize location information.

***Section 3. Protection against Retaliation***

Covered entities cannot take adverse action against an individual for exercising rights under this chapter, unless location data is essential to the provision of the good, service, or service feature that the individual requests, and then only to the extent that such data is essential.

This prohibition includes but is not limited to:

- Refusing to provide a good or service to the individual;
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; or
- Providing a different level or quality of goods or services to the individual.

***Section 4. Enforcement***

A violation of this chapter or a regulation under this chapter regarding an individual's location information constitutes an injury to that individual and shall be deemed an unfair or deceptive act or practice in the conduct of trade or commerce under chapter 93A.

Any individual alleging a violation of this chapter by a covered entity or service provider may bring a civil action in the superior court or any court of competent jurisdiction; provided that, venue in the superior court shall be proper in the county in which the plaintiff resides or was located at the time of any violation.

The court may award:

- Actual damages, including damages for emotional distress, or $5,000 per violation, whichever is greater,
- Punitive damages; and
- Any other relief, including but not limited to an injunction or declaratory judgment, that the court deems to be appropriate.

The Attorney General may bring an action pursuant to section 4 of chapter 93A against a covered entity or service provider to remedy violations of this chapter and for other relief that may be appropriate.

***Section 5. Implementation***

The Attorney General may adopt, amend or repeal rules and regulations for the implementation, administration, and enforcement of this chapter.

**SECTION 3: Location Information Collected Before Effective Date**

Location information collected, processed, and stored prior to the effective date of this Act shall be subject to subsections 2(e)(3), 2(e)(5), and 2(f) of Chapter 93N.

**SECTION 4: Effective Date**

This Act shall take effect 1 year after enactment.