**Bill Number:** H. 78
**Title:** *An Act establishing the Massachusetts consumer data privacy act*
**Lead Sponsor:** Representative Tricia Farley-Bouvier
**Hearing Date:** April 9, 2025
**Report Date:** June 8, 2025
**Current Law:**

- **M.G.L. Chapter 66A** regulates government uses and protection of personal information.
- **M.G.L. Chapter 76 § 1** defines "private school" as used in the bill.
- **M.G.L. Chapter 93 § 42** defines "trade secret" 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:** H. 78 inserts the MCDPA as a new chapter of the Massachusetts General Laws. The MCDPA requires data minimization, which means that data holders ("controllers") must limit the collection, processing, or transfer of consumer's personal data to what is adequate, relevant, and reasonably necessary to provide their services. Data minimization includes deleting or removing information when it is no longer necessary to mitigate the misuse of personal information and risks associated with data breaches. The bill requires additional protections for a consumer's sensitive data – health information, financial information, specific geolocation information, etc. Mandates clear, affirmative, informed consent (opt-in) for sensitive data transfers and has a blanket prohibition on the sale of sensitive data or processing the data of minors for targeted advertising (similar to Maryland). The bill also requires data protection assessments for high-risk processing activities, with reports submitted to the Attorney General with summaries of such assessments made accessible to the public. The MCDPA also includes a private right of action as a means of enforcement and includes Attorney General rulemaking.

**Legislative History:** New File

**Section 1. Definitions**

Includes specifications for targeted advertising. "Targeted advertising" means displaying to an individual or device identified by a unique persistent identifier an online advertisement that is selected based on known or predicted preferences, characteristics, behavior, or interests

associated with that individual or device. It does not include first-party advertising or contextual advertising.

“Contextual advertising” means displaying an advertisement that not vary based on the identity of the individual recipient and is based on the immediate content of a webpage on which the advertisement appears, a specific request of a consumer for information or feedback, or a consumer’s immediate presence in a geographic area with a radius no smaller than 10 miles.
“First-party advertising” means processing by a first party of its own data for the purposes of advertising that is carried out through direct communications with a consumer, in a physical location operated by the first party, or through display of an ad on the first party’s own website, app, or other online content. A “first party” is defined as a consumer-facing controller with which the consumer intends or expects to interact.

“Consumer health data” means any personal data that a controller describes or reveals a consumer's past, present, or future physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data

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

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

“Gender-affirming health care services” means all medical care relating to the treatment of gender dysphoria as set forth in the most recent edition of the American Psychiatric Association's “Diagnostic and Statistical Manual of Mental Disorders” and gender incongruence, as defined in the most recent revision of the “International Statistical Classification of Diseases and Related Health Problems.”

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

“Minor” means any consumer who is younger than 18 years of age.

“Precise geolocation data” means information derived from technology, including, but not limited to, latitude and longitude coordinates from global positioning system mechanisms or other similar positional data, that reveals the past or present physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals with precision and accuracy within a radius of one thousand seven hundred fifty feet.

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

“Reproductive or sexual health care” means any health care-related services or products rendered or provided concerning a consumer's reproductive system or sexual well-being, including, but not limited to, any such service or product rendered or provided concerning

(A) an individual health condition, status, disease, diagnosis, diagnostic test or treatment,

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

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

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

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

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

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

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

“Sensitive data” means personal data that includes:

(A) data revealing racial or ethnic origin, color, national origin, religious beliefs, mental or physical health condition or diagnosis, status as pregnant, sex life, sexual orientation, status as transgender or non-binary, philosophical beliefs or union membership, status as a military servicemember or veteran, income level or indebtedness, or citizenship or immigration status;

(B) consumer health data;

(C) genetic or biometric data;

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

(E) precise geolocation data;

(F) 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;

(G) the online activities of a consumer (or device linked or reasonably linkable to a consumer) over time and across websites, online applications, or mobile applications that do not share common branding, or data generated by profiling performed on such data;

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

(I) status as a victim of a crime.

**Section 2. Applicability**
Applies to businesses operating in Massachusetts or targeting Massachusetts residents that (a) collect/process data from at least 25,000 consumers (not counting certain transaction information needed to complete sales) or (b) derive any revenue from selling personal data. The payment transaction exemption allows businesses to process data solely for completing payments if deleted within 90 days.

**Section 3. Scope**
Outlines specific exemptions to the law, including government entities and certain types of protected health information. Exempts various categories of data already regulated by federal laws like HIPAA, Gramm-Leach-Bliley Act, and Family Educational Rights and Privacy Act. The section also clarifies that compliance with COPPA's parental consent requirements satisfies this law's parental consent obligations.

**Section 4. Consumer Rights (data subject rights)**
Consumers are granted several rights over their data, including the right to confirm data collection, access their data, correct inaccuracies, delete their data, and opt out of targeted advertising. Controllers must respond to consumer requests within 45 days. The section includes specific provisions for authenticating requests and handling appeals. Information provided in response to a consumer request shall be provided by a controller, free of charge, up to two times per consumer during any twelve-month period.

- Right to Access
    - Individuals have the right to confirm whether or not a controller is collecting or processing personal data. If the covered entity transfers this data to any third parties, then the consumer is also able to request a list of third parties that the controller has transferred data to.
- Right to Correct
    - Individuals may request to correct any inaccurate 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 personal data that is provided by, or obtained about, the consumer, including personal data the consumer provided to the controller, data the controller obtained from another source, and any derived data.
    - Individuals may instruct the covered entity to notify all third parties of the individual’s deletion request.
- Right to Transport
    - Individuals may request an export copy of their personal data collected or processed by the controller in a portable and readily usable format that allows the consumer to transmit the data elsewhere.

- Right to Opt Out

- Individuals have the right to opt out of the collection and processing of personal data for the purposes of targeted advertising or for the profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.
- Individuals have the right to opt out of the transfer of personal data.

**Section 5. Authorized Agent**
Allows consumers to designate authorized agents to exercise their rights under the law on their behalf. Controllers must verify both the identity of the consumer and the authority of the agent. The section ensures consumers can delegate their privacy rights while maintaining security.

**Section 6. Actions of Controllers**
Controllers must limit data collection to what's necessary based on the sensitivity of the data, implement reasonable data security practices, and obtain the consumer's affirmative consent before transferring sensitive data. They must provide clear privacy notices and cannot discriminate against consumers who exercise their rights. The section requires controllers to offer easy-to-use opt-out mechanisms, including honoring opt-out preference signals.

Except with respect to sensitive data, a controller may process or transfer personal data collected under this subsection to provide first-party advertising or targeted advertising; provided, however, that this paragraph does not permit the processing or transfer of personal data for targeted advertising to a consumer who has opted out of such advertising.

Controllers may not sell sensitive data, sell children's data, or process children's data for the purpose of targeted advertising.

Controllers must provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes:

- Categories of personal data collected (including sensitive data)
- Purpose for collecting each category of data
- How consumers can exercise their rights
- Categories of personal data transferred to third parties
- Categories of third parties receiving personal data
- Data retention timeframes or criteria for determining retention
- Contact method for consumers (email address)

If any material changes are made to such privacy notices, controllers must notify affected consumers before implementing changes and allow consumers the opportunity to withdraw or renew consent.

Controllers must establish one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this chapter, including an opt out mechanism to opt out of targeted advertising, the sale of data, and profiling for automated decisions.

**Section 7. Responsibilities of Processors and Controllers**

Establishes the relationship and obligations between processors and controllers through mandatory contractual provisions. Processors must follow controllers' instructions and help them comply with the law's requirements. Includes specific security requirements and clarifies when a processor might be considered a controller.

**Section 8. Data Protection Assessments**
Controllers must conduct and document data protection assessments for high-risk processing activities, including targeted advertising and processing sensitive data. These assessments must be submitted to the Attorney General within 30 days and be publicly available. Data protection assessments must be conducted before controllers may initiate processing that present's a heightened risk. The section requires regular reviews and updates of these assessments throughout the processing activity's lifecycle.

The bill defines processing that presents a heightened risk of harm to a consumer as: "the collection or processing of personal data for the purposes of targeted advertising; *the sale of personal data*; the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of: unfair or deceptive treatment of, or unlawful disparate impact on, consumers, financial, physical or reputational injury to consumers, 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 other substantial injury to consumers; *and the collection or processing of sensitive data*."

**Section 9. De-identified Data**
Controllers are encouraged to de-identify data to allow for research and analysis while still protecting consumer privacy. Controllers must take technical measures to ensure de-identified data cannot be re-associated with individuals and publicly commit to maintaining it in de-identified form. Requires contractual obligations for recipients of de-identified data to comply with provisions of this act and requires controllers to exercise oversight over recipients of pseudonymous or de-identified data and take appropriate steps to address any breaches of those contractual commitments.

The section includes oversight requirements for controllers transferring de-identified data.

**Section 10. Limitations**
This section outlines various exemptions allowing controllers to process data for specific purposes like law enforcement, research, and security. It protects privileged communications and First Amendment rights. The section requires that any exempt processing must be reasonable, necessary, and proportionate to the stated purpose.

**Section 11. Rulemaking**
The Attorney General is authorized to adopt rules and regulations to implement the Act. This provides flexibility for addressing new technologies and challenges. The section is brief but important for ensuring the law can adapt to changing technological circumstances.

**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 the Massachusetts Consumer Protection Law (MGL Ch. 93A).

Includes a private right of action for consumers alleging violations of the chapter. The court may award:

- Liquidated damages of not less than $15,000 per individual per violation (adjusted for inflation),
- Punitive damages,
- Injunctive relief,
- Declaratory relief, and
- Reasonable attorney's fees and costs

The Attorney General can also bring civil actions with penalties of at least $15,000 per individual per violation. As in the private right of action, other remedies, including injunctive relief, are also available. Courts can consider various factors when calculating penalties, including the severity of violations and the defendant's privacy record. The section prohibits contractual waivers of consumer rights.

**Section 13. Relationship to Other Laws**
Clarifies that this act does not limit the rights or responsibilities established by other privacy laws in Massachusetts.

**Section 14. Targeted Advertising to Minors**
A covered entity may not engage in targeted advertising to minors.

**Section 15. Additional Protections for Location Information.**
Requires that specific geolocation information of visitors to the Commonwealth is treated the same way as resident's location information.