Bill Number: H.80
Title: An Act establishing Comprehensive Massachusetts Consumer Data Privacy Act
Lead Sponsor: Representative Kate Hogan
Hearing Date: April 9, 2025
Report Date: June 8, 2025
See Senate Filing: S.33

Current Law:

- **M.G.L. Chapter 9A § 1** defines "gender-affirming health care services" as used in the bill.
- **M.G.L. Chapter 66** regulates public records in Massachusetts.
- **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 § 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.

Executive Summary: Grants consumers rights to access, correct, delete, and opt out of the sale of their personal data, particularly sensitive data including health information. It applies to businesses that process data of 100,000+ consumers or 25,000+ consumers while deriving over 25% of revenue from data sales, with special protections for minors and additional safeguards around reproductive and gender-affirming healthcare data. Controllers must conduct data protection assessments for high-risk processing activities, and implement technical security measures to protect data. The law includes specific provisions banning geofencing near mental health or reproductive health facilities and requires new mechanisms for consumers to opt out of targeted advertising and profiling. Enforcement falls exclusively to the Attorney General, and until December 31, 2027, the Attorney General would be obligated to provide potential violators with a 60 day opportunity to cure before bringing a lawsuit.

Legislative History: New File

Section 1.
"Consumer Health Data", means any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.

"Consumer Health Data", means any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.

"Gender-affirming health care services" shall have the same meaning as provided in section 1 of chapter 9A of the General Laws as amended by chapter 127 of the Acts of 2022.

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

“Heightened risk of harm to minors”, processing minors' personal data in a manner that presents any reasonably foreseeable risk of

(A) any unfair or deceptive treatment of, or any unlawful disparate impact on, minors,
(B) any financial, physical or reputational injury to minors, or
(C) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of minors if such intrusion would be offensive to a reasonable person.

“Mental health facility”, any health care facility in which at least seventy per cent of the health care services provided in such a facility are mental health services.

“Minor”, any consumer who is younger than eighteen years of age.

"Precise geolocation data", information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. "Precise geolocation data" does not include: (i) the content of communications; or (ii) any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

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

“Reproductive or sexual health facility”, any health care facility in which at least seventy per cent of the health care-related services or products rendered or provided in such facility are reproductive or sexual health care.

"Sensitive data", personal data that includes

(A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual,

(C) personal data collected from a known child

(D) precise geolocation data

(E) status as transgender or nonbinary

(F) consumer health data; or

(G) data concerning an individual's status as a victim of a crime.

"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. "Targeted advertising" does not include (A) advertisements based on activities within a controller's own Internet web sites or online applications, (B) advertisements based on the context of a consumer's current search query, visit to an Internet web site or online application, (C) advertisements directed to a consumer in response to the consumer's request for information or feedback, or (D) processing personal data solely to measure or report advertising frequency, performance or reach.

Section 2.

Applies to businesses operating in Massachusetts or targeting Massachusetts residents that (A) controlled or processed the personal data of not less than one hundred thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (B) controlled or processed the personal data of not less than twenty-five thousand consumers and derived more than twenty-five per cent of their gross revenue from the sale of personal data.

- Excludes personal data controlled solely for payment transaction purposes

Section 3.

Outlines specific exemptions to the law, including for government entities, institutions of higher education, financial institutions subject to the Gramm-Leach-Bliley Act (GLBA), national securities associations, and those contracted to process certain types of protected health information.

Additionally exempts various categories of data already regulated by federal laws like HIPAA, GLBA, Fair Credit Reporting Act, Driver's Privacy Protection Act and Family Educational Rights and Privacy Act. Also clarifies that compliance with COPPA's parental consent requirements satisfies this law's parental consent obligations.

Section 4.

Consumers are granted certain rights over their data: the rights to confirm their data is being collected and access said data, to correct inaccuracies, to delete their data, to obtain copies of

their data, and to opt out of targeted advertising and profiling. Controllers must respond to consumer requests within 45 days (with a possible 45 day extension) and provide the information free of charge once per year per consumer.
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, twice 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 sale of personal data, except as provided in subsection (b) of section 6 of this act.

A controller that has obtained personal data about a consumer from a source other than the consumer (such as purchasing third-party data) shall be deemed in compliance with a consumer's request to delete such data by 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 data for any other purpose.

Section 5.
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 allows consumers to delegate their privacy rights while maintaining the security guidelines of this chapter.

Section 6.
Mandates that data collectors limit their collection to information that is adequate, relevant, and necessary for explicitly disclosed purposes (similar to the Connecticut Data Privacy Act and other state privacy laws). Controllers must obtain consumer consent before processing data for purposes beyond the original disclosure. Controllers are required to establish robust administrative, technical, and physical data security practices to protect personal information's confidentiality and integrity.

Requires explicit consumer consent for processing sensitive data. Provides additional safeguards for children's data, mandating compliance with existing child protection regulations like COPPA. The provision also prohibits data processing that could result in unlawful discrimination against consumers.

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)

By July 1, 2025, controllers must allow consumers to opt out of having their data processed for the purposes of targeted advertising or sale through an opt out preference signal sent by a platform, technology, or other such mechanism. This mechanism must require affirmative consent and be consumer-friendly and as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation.

- A controller that recognizes opt out preference signals that have been approved by other state laws or regulations shall be deemed to be in compliance with subsection (A) of this section.
- If a controller responds to consumer opt-out requests received by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered for the retention, use, sale or sharing of the consumer's personal data.

Bans the use of a geofence to establish a virtual boundary that is within 1,750 feet of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking,

collecting data from or sending any notification to a consumer regarding the consumer's consumer health data; or sell, or offer to sell, consumer health data without first obtaining the consumer's consent.
Section 7.

Controllers must use reasonable care to avoid any heightened risk of harm to minors caused by their online service, product or feature. In any enforcement action brought by the Attorney General pursuant to this act, there shall be a rebuttable presumption that a controller used reasonable care as required under this section if the controller complied with the provisions of this act concerning data protection assessments.

Controllers may not sell children's data, or process children's data for the purpose of targeted advertising or for profiling in furtherance of any fully automated decision made by such controller that produces any legal or similarly significant effect. Limits the collection of minors' precise geolocation data to necessary purposes only

Controllers must obtain the minor's consent or, if the minor is younger than thirteen years of age, the consent of such minor's parent or legal guardian. A controller that complies with the verifiable parental consent requirements established in the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., shall be deemed to have satisfied any requirement to obtain parental consent under this subdivision. This section also prohibits the use of any design features that substantially subvert user autonomy or choice.

Requires easy-to-use safeguards limiting unsolicited communications from adults to minors, with exemptions from some requirements for certain services like email and direct messaging.

Section 8.
Requires processors to adhere to controller instructions and assist with meeting obligations under this section. Requires assistance with security obligations and breach notifications under Chapter 93H of the General Laws. Outlines the contractual requirements for controllers and processors which include:

- Mandating appropriate technical measures to fulfill consumer rights requests
- Mandating confidentiality duties for all persons processing personal data
- Requiring processors to delete or return all personal data at the controller's direction
- Specifying that subcontractors must meet the same obligations as processors

Section 9.
Requires controllers to conduct and document data protection assessments for high-risk processing activities after January 1, 2024 (not retroactive).

Controllers must 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. Processing that presents a heightened risk of harm to a consumer includes:

- Processing of personal data for the purposes of targeted advertising

- The sale of personal data
- Processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of discrimination against the consumer, , financial, physical or reputational injury to the consumer, an invasion of the consumer's privacy, or other substantial injury to the consumer
- Processing of sensitive data

Data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks.

For controllers that offer services to minors, assessments must include the categories of minors' personal data that such online service, product or feature processes, the purposes for which such controller processes minors' personal data with respect to such online service, product or feature, and any heightened risk of harm to minors that is a reasonably foreseeable result of offering such online service, product or feature to minors.

The Attorney General may evaluate data protection assessments for compliance with the aforementioned responsibilities. Data protection assessments will be confidential and shall be exempt from disclosure under the Public Records Act, as set forth in chapter 66 of the General Laws. Controllers must make data protection assessments available to the Attorney General.

Controllers that conduct data protection assessments in compliance with other applicable laws or regulations can be in compliance with this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section. Allows single assessments for comparable processing operations.

Section 10.
Requires controllers with de-identified data to take reasonable measures preventing re-identification. Mandates public commitment to maintain and use de-identified data without re-identification attempts. Requires contractual obligations for recipients of de-identified data to comply with all provisions of Section 1 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. Further exempts pseudonymous data from certain consumer rights requests.

Section 11.
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 12.
Grants the Attorney General exclusive enforcement authority. Explicitly prohibits private rights of action.

Establishes a 60-day cure period expiring December 31, 2027. Designates violations as unfair trade practices under Chapter 93A.

Requires the Attorney General to submit a report on violations by February 2027 that includes: the number of notices of violation the Attorney General has issued, the nature of each violation, the number of violations that were cured during the sixty-day cure period, and any other matter the Attorney General deems relevant for the purposes of such report.

Includes factors to consider when granting cure opportunities after January 2028 such as the number of violations, the size and complexity of the controller or processor, the nature and extent of the controller's or processor's processing activities, the substantial likelihood of injury to the public, the safety of persons or property, whether such alleged violation was likely caused by human or technical error.

Section 13.
Establishes July 1, 2026 as the effective date.