



MASSACHUSETTS DATA PRIVACY AND PROTECTION ACT (MDPPA)

Reps. Vargas & D. Rogers (H.83) & Sen. Creem (S.25)

BACKGROUND

The Massachusetts Data Privacy and Protection Act is based on a bipartisan bill proposed in Congress in 2022, the American Data Privacy and Protection Act (“ADPPA”). The bill went through extensive negotiations between members of Congress of both parties, industry, civil rights groups, and consumer protection and privacy groups. The ADPPA received overwhelming bipartisan support in the House Energy & Commerce Committee, where it was favorably approved on a 53-2 vote. Unfortunately, Congress failed to enact ADPPA, but Massachusetts legislators can now take advantage of the outcome of those negotiations by modeling a state bill on the bipartisan consensus language in ADPPA. The Massachusetts Data Privacy and Protection Act provides that opportunity.

KEY PROVISIONS

- **Data minimization:** Establishes limits on the unfettered processing of personal data by setting a baseline requirement that entities only collect, use, and transfer data that is reasonably necessary and proportionate to provide or maintain a product or service requested by the individual (or pursuant to certain enumerated purposes.)
- **Strict restrictions on sensitive data collection and use:** Sets heightened protections for collection and use of sensitive data (i.e., biometrics, geolocation, health data), which is only permitted when strictly necessary and not permitted for advertising purposes.
- **Civil Rights:** Extends civil rights to online spaces by prohibiting entities from processing data in a way that discriminates or otherwise makes unavailable the equal enjoyment of goods and services on the basis of race, color, religion, national origin, sex, sexual orientation, gender, or disability.
- **Cross-context behavioral advertising prohibited:** The collection, use, and transfer of information identifying an individual’s online activities over time and across third party websites and services is strictly limited and cannot be used for advertising.
- **Protections for children and teens:** Prohibits targeted advertising to minors under age 17. Personal data of minors is considered “sensitive data.” These additional protections would only apply when the covered entity knows the individual in question is under age 17, though the standard for certain high-impact social media companies is “known or should have known,” and for large data holders is “knew or acted in willful disregard of the fact that the individual was a minor.”
- **Algorithmic fairness and transparency:** Requires large data holders to conduct algorithmic impact assessments, which include mitigation measures to avoid potential harms from the algorithms. Entities must also conduct algorithm design evaluations prior to deployment in some instances. The assessments and evaluations must be submitted to the Attorney General. A summary must be posted publicly.

- **Manipulative design restrictions:** Prohibits obtaining consent in ways that are misleading or manipulative (e.g., dark patterns). Prohibits deceptive advertising.
- **Individual Rights:** Gives consumers the rights to access, correct, and delete personal information about them. Consumers also have the right to opt out of both data transfers to third parties and targeted advertising. Also requires the Attorney General to recognize, and entities to honor, global opt-out mechanisms.
- **Service Providers:** Establishes requirements for service providers handling personal data, including a prohibition on commingling data from multiple covered entities. Service providers can only collect, process, and transfer data to the extent necessary and proportionate to provide service requested by covered entity.
- **Data Brokers:** Data Brokers must register with the Office of Consumer Affairs and Business Regulation. The OCABR will create a public registry of data brokers.
- **Small business protections:** Small businesses (as defined) are exempt from compliance with many provisions of the Act.
- **Executive responsibility:** An executive must personally certify each entity's compliance with the Act.
- **Enforcement:** The Attorney General may bring cases in court to remedy violations of this chapter and for other relief that may be appropriate.
- **Private Right of Action:** Individuals may enforce their rights under the Act by bringing a case against a covered entity seeking liquidated damages, punitive damages, injunctive relief, reasonable attorney's fees and litigation costs, and any other appropriate relief. Small businesses are exempt from this provision.
- **Rulemaking:** The Attorney General is empowered to issue regulations for purposes of carrying out the Act.
- **Adds workplace surveillance protections:** Though not originally addressed in ADPPA, the Massachusetts Data Privacy and Protection Act adds section 204 to the labor code, establishing protections for workers against electronic monitoring.