



LEGAL UPDATES

Minnesota Enacts Comprehensive Data Privacy Law

07/10/2024 | 5 minute read

Minnesota has become the 19th state to pass a comprehensive data privacy law. On May 24, Governor Tim Walz signed into law the Minnesota Consumer Privacy Act (H.F. 4757) (the "MCPA"), which takes effect July 31, 2025.

State legislation continues to fill the void left in the absence of a comprehensive federal privacy law. Businesses and organizations that handle personal data must comply with multiple federal sectoral, state and sometimes global data privacy laws.

Who Is Covered?

The MCPA covers legal entities that conduct business in Minnesota or produce products or services targeted to state residents and that satisfy one or more of the following:

- during a calendar year, control or process the personal data of at least 100,000 consumers (excluding payment transactions)
- derive over 25% of gross revenue from the sale of personal data and processes or controls the personal data of at least 25,000 consumers.

MCPA Definitions

Personal data is defined as "any information that is linked or reasonably linkable to an identified or identifiable natural person." Personal data does not include deidentified data or publicly available information. "Publicly available information" means information that (1) is lawfully made available from federal, state, or local government records or widely distributed media, or (2) a controller has a reasonable basis to believe has lawfully been made available to the general public.

The MCPA uses the term "controller" which is like the definition that appears in the General Data Protection Regulation (GDPR) and other data privacy laws. Controller means the "natural or legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data."

Related People

Michael (Mike) R. Cohen, PLS, CIPP/US, CIPP/E, CIPM, FIP

Counsel

Minneapolis

612.632.3345

michael.cohen@lathropgpm.com

Tedrick A. Housh, III, CIPP/US, CIPP/E

Partner

Kansas City

816.460.5642

tedrick.housh@lathropgpm.com

Alexandra Bass

Associate

Chicago

816.460.5831

alexandra.bass@lathropgpm.com



The MCPA defines “consumer” as a natural person who is a Minnesota resident acting only in an individual or household context. Consumer does not include a natural person acting in a commercial or employment context. This means that the MCPA does not apply to personal data relating to job applicants, employees, and individuals acting in their capacity as business representatives.

For the purposes of the MCPA a “sale” includes an exchange of personal data for monetary consideration or “any other valuable consideration.”

The MCPA specifically applies to “technology providers” that contract with public education agencies and institutions pursuant to Minnesota Statute § 13.32.

MCPA Exemptions

The MCPA includes exemptions for certain types of businesses and data. Governmental entities, federally recognized Indian tribes, “small business” as defined by the U.S. Small Business Administration regulations, air carriers under the Airline Deregulation Act, and certain kinds of banks, credit unions and insurance companies are exempt.

Unlike the California Consumer Privacy Act (“CCPA”) and other state data privacy laws, there is no broad exemption for non-profits. Non-profits are exempt if they are “established to detect and prevent fraudulent acts in connection with insurance.” The MCPA does not include an entity-level exemption for companies that are covered entities or business associates under HIPAA.

The data-level exemptions are consistent with most other state privacy laws. Specifically, the Minnesota Act exempts data regulated by HIPAA, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Driver’s Privacy Protection Act, the Family Educational Rights and Privacy Act, the Farm Credit Act, the Minnesota Insurance Fair Information Reporting Act, and various other regulations.

Enhanced Privacy Rights for Consumers

The MCPA contains obligations for controllers that largely follow provisions in other comprehensive state privacy laws.

Provisions similar to other state laws include recognition of universal opt-out mechanisms, required data protection assessments, exclusive attorney general enforcement, and a 30-day right to cure that sunsets in 2026.

The MCPA provides consumers with the right to:

- Confirm whether a controller is processing personal data about the consumer and to access the categories of personal data processed by the controller;
- Correct inaccurate personal data concerning the consumer, taking into account the nature of the data and purposes of processing;
- Delete the consumer’s personal data (subject to exceptions);
- Obtain a copy of personal data that the consumer previously provided to the controller, where the data processing is conducted by automated means; and
- Obtain a list of the specific third parties to whom the controller disclosed the consumer’s personal data or, if not available, a list of the specific third parties to whom the controller has disclosed **any** consumers’ personal data.

How is MCPA Different?

Profiling

The law includes new consumer rights and business obligations around profiling practices. Consumers can request information regarding a profiling decision carried out against them, including the reasoning behind a particular profiling decision and access to the data used to reach the decision.

A profiled consumer “has the right to question the result of the profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future.” A consumer also has the “right to review the consumer’s personal data used in the profiling” and, if “the decision is determined to have been based upon inaccurate personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.”

Data Inventory

The controller may need to maintain a data inventory and document its policies and procedures used for data security and to comply with the law.

Minnesota is the first state to require businesses to maintain such data inventories.

The law states that a “controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data, **including the maintenance of an inventory of the data that must be managed to exercise these responsibilities.** The data security practices shall be appropriate to the volume and nature of the personal data at issue.”

Data Retention

The new law provides that a controller may not retain personal data that is no longer relevant and reasonably necessary in relation to the purposes for which the data were collected and processed, unless retention of the data is otherwise required by law or permitted under a statutory exception such as performing a contract to which a consumer is a party, fulfilling the terms of a written warranty, and others specifically listed in the MCPA.

Must Document Compliance

A business must “document and maintain a description of the policies and procedures that controller has adopted to comply” with the law. The description must include the name and contact information for the controller’s chief privacy officer or other individual with primary responsibility for directing the policies and procedures implemented to comply with the law.

Data Protection Assessments

The MCPA requires a controller to conduct “data privacy and protection assessments” for certain processing activities, including processing personal data in connection with targeted advertising, sales of personal data, processing sensitive data, profiling that presents a heightened risk of harm to consumers and profiling that presents certain types of foreseeable risks (e.g., unfair and deceptive treatment, financial or reputational injury, intrusion on seclusion, etc.). The



controller needs to document and retain such assessments and make them available to the Minnesota Attorney General upon request.

Enforcement

The MCPA is enforceable by the Attorney General's office. There is no private right of action. Violations of the MCPA are subject to injunctive relief and civil penalties up to \$7,500 per violation. The Minnesota Attorney General is required to provide a controller or processor with notice of the specific provisions of the MCPA that it alleges have been violated and 30 days to cure the violations prior to bringing an enforcement action. This cure provision expires on January 31, 2026.

Effective Date

The law's effective date is July 31, 2025. Postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029.

If you have any questions regarding compliance with the MCPA or any other state, federal, or global data privacy law or regulation please reach out to [Michael Cohen](#), [Tedrick Housh](#), [Alexandra Bass](#) or your regular Lathrop GPM contact.

More information on data privacy and security laws can be found in our [Legal Guide to Privacy and Data Security](#).