Skol, Vikings: Minnesota Enhances Consumer Data Protections

On May 24, Minnesota Governor Tim Walz approved the Minnesota Consumer Data Privacy Act (MCDPA), making Minnesota the nineteenth state to pass comprehensive consumer data privacy legislation.

The MCDPA largely matches data privacy protections enacted in other states, particularly those in Colorado, Connecticut, and Virginia. The MCDPA contains several unique provisions, however, including a novel definition of specific geolocation data, a right to question the results of profiling decisions that produce significant effects, and a requirement to maintain a data inventory. These distinctive provisions will necessitate additional compliance steps even for those already complying with other consumer data privacy laws.

The MCDPA will be effective beginning July 31, 2025, though post-secondary institutions regulated by the Office of Higher Education need not comply until July 31, 2029.

Applicability

Threshold

The MCDPA applies to legal entities that conduct business in Minnesota or produce products or services targeting Minnesota residents and meet one of two of the below threshold provisions during the immediately-preceding calendar year:

1. The entity controls or processes the personal data of at least 100,000 Minnesota consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction**.**
2. The entity controls or processes the personal data of at least 25,000 Minnesota consumers **and** derives over 25% of its gross revenues from the sale of personal data.

As with most other consumer data privacy laws, the definition of “consumer” excludes a natural person acting in a commercial or employment context.

Exemptions

In addition to exempting employee and contractor information, the MCDPA enumerates several entity-level and data-level exemptions. The law does not apply to government entities, state- or federally-chartered banks, insurance companies, airlines, covered entities or business associates as defined by the Health Insurance Portability and Accountability Act (HIPAA), and federally-recognized American Indian tribes. Similar to state privacy laws in Texas and Nebraska, the MCDPA excludes small businesses, yet prohibits small businesses from selling consumers’ sensitive data without their consent—regardless of the number of consumers whose data they process. Minnesota notably follows the trend of Oregon, Colorado, and Delaware, which do not generally exempt nonprofits. Like Delaware, however, Minnesota does provide a limited exemption for nonprofit entities established to detect and prevent acts of insurance fraud.

The MCDPA largely tracks legislation in other states by providing standard data-level exemptions for personal information already protected pursuant to research conducted in accordance with federal regulations governing clinical human subjects research, the Fair Credit Reporting Act, HIPAA, the Gramm-Leach-Bliley Act (GLBA), the Driver's Privacy Protection Act, the Farm Credit Act, and the Family Educational Rights and Privacy Act.

Consumer Rights

Though it fundamentally mirrors other states' privacy laws, the MCDPA includes several provisions in its list of consumer rights that set it apart.

Like Oregon, Minnesota grants consumers the right to obtain a list of the specific third parties to whom the controllers have disclosed their personal data. Like Nebraska and New Jersey, Minnesota also requires controllers to recognize universal opt-out mechanisms (UOOMs), whereupon consumers may opt out of any processing of their personal data for sales and targeted advertisement.

Minnesota follows the example of consumer-friendly Kentucky and Connecticut in its definition of "biometric data." Under the MCDPA, the definition of biometric data does not include digital or physical photographs, audio or video recordings, or data generated therefrom, unless it is generated to identify a specific individual.

Minnesota departs from the pack by adopting a new definition for "specific geolocation data." While other states describe it as a radius measuring a certain distance, the MCDPA defines "specific geolocation data" as GPS-level latitude and longitude, other mechanisms that directly identify the geographic coordinates of a consumer or device, or a street address derived therefrom.

The MCDPA also distinguishes itself by providing consumers the right to opt out of profiling that results in decisions that produce legal effects or similarly significant effects concerning the consumer; question the results of profiling; be informed of the reasons behind a specific profiling decision; and, if feasible, be informed of what actions the consumer might have taken to secure a different decision and the actions the consumer might take to secure a different decision in the future.

Controller Obligations

Minnesota is the first state to require controllers to maintain data inventories. Controllers must "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect confidentiality, integrity, and accessibility of personal data[.]" In addition, but consistent with other states, controllers also must conduct "data privacy and protection assessments" to identify the risks and benefits of their activities.

Controllers are limited in how they can use consumer data under the MCDPA. The underlying purpose must be "adequate, relevant, and reasonably necessary." Controllers may collect, process and share data only where strictly necessary to provide consumer-requested products or services. The MCDPA markedly includes a prohibition against processing consumers' personal data on the basis of actual or perceived race, color, sexual orientation, familial status, or other sensitive demographics. Similar to Maryland and New Jersey, Minnesota adopts extra protections for children's personal data.

The MCDPA also imposes a unique requirement that controllers document and maintain a description of the policies and procedures that they adopt to comply with the law. Controllers must include the name and contact information of the chief privacy officer, or other individual with primary responsibility for compliance, and must describe any policies and procedures designed to address the following:

1. Reflect the requirements of the MCDPA in the design of the controllers' systems.
2. Identify and provide personal data to a consumer as required by the MCDPA.
3. Establish, implement, and maintain reasonable security safeguards, including maintenance of the aforementioned inventory of data subject to such safeguards.
4. Comply with data minimization requirements.
5. Prevent the retention of personal data for longer than reasonably necessary or when no longer relevant for the purpose for which it was collected, unless otherwise required or permitted by law.
6. Identify and remediate violations of the MCDPA.

Enforcement

The MCDPA does not create a private right of action. Instead, the Minnesota Attorney General's Office holds the exclusive power to enforce the law. The attorney general may bring civil actions against controllers or processors, who face a penalty of up to $7,500 per violation. For any violation occurring on or before January 31, 2026, however, the Attorney General must provide notice through a warning letter and a 30-day period to cure. This provision matches the one found in Kentucky's comprehensive privacy law and aligns with those in other states, whose cure periods typically range from thirty to ninety days.

Important Dates

- **July 31, 2025**: The MCDPA goes into effect.
- **January 31, 2026**: The right to cure sunsets.
- **July 31, 2029**: Post-secondary institutions regulated by the Office of Higher Education must comply with the MCDPA.

Our team will continue to monitor the MCDPA. If you have any questions about this or any other state privacy laws and how they could affect your business, please contact the authors.

The authors wish to thank summer associate Alessandro Colangelo for his contributions to this content.