Published on *The National Law Review* https://natlawreview.com

The Gopher State Goes for It: Minnesota Passes Consumer Data Privacy Law

Article By:

David P. Saunders

James S. Mann

Consult our interactive state privacy law map to learn more about all of the enacted state consumer privacy laws.

On May 19, 2024, the Minnesota Legislature passed a comprehensive privacy bill, sending the Minnesota Consumer Data Privacy Act (MCDPA) to Governor Tim Walz's desk for signature into law.

The law, which would take effect July 31, 2025 (except for postsecondary institutions, which could have until July 31, 2029), is similar to prior state consumer privacy laws but with several twists. These differences will require additional compliance steps for companies that might have been subject to previously implemented state consumer privacy laws.

IN DEPTH

WHO DOES MCDPA APPLY TO?

MCDPA applies to any person that conducts business in Minnesota or provides products or services that are targeted to Minnesota residents *and*, during the immediately preceding calendar year, either:

1. Controlled or processed the personal data of at least **100,000** Minnesota consumers (excluding that personal data controlled or processed solely for the purpose of completing a payment transaction); ***or***

2. Controlled or processed the personal data of at least **25,000** Minnesota consumers and derives more than **25%** of their gross revenue from the sale of personal data.

These conditions track with what had been (before the recent trend of state consumer privacy laws) the norm from the Connecticut and Virginia models. However, MCDPA also applies to technology providers under Minnesota's educational data laws (*i.e.*, entities that provide technology to schools).

WHO IS A "CONSUMER"?

MCDPA follows the majority of other states and defines a consumer to be an individual who is a resident of Minnesota acting only in the individual context (*i.e.*, excluding employment or commercial actors).

WHAT IS "PERSONAL DATA"?

The definition of "personal data" looks familiar as well: information that is linked or reasonably linkable to an identified or identifiable natural person but excluding de-identified data or publicly available information.

WHO CAN ENFORCE?

Minnesota's attorney general has exclusive enforcement power. With respect to an alleged violation on or before January 31, 2026, the attorney general must provide a warning letter and a 30-day cure period prior to initiating any action. Civil penalties can be up to $7,500 per violation.

WHO IS EXEMPT?

MCDPA includes a short list of entity-level exemptions, including for government entities, certain financial entities such as banks and insurance companies, small businesses, airlines and federally recognized American Indian tribes. Minnesota continues the state-law trend of applying to nonprofits *unless* the entity is engaged in certain conduct (here, to detect and prevent fraudulent acts in connection with insurance).

MCDPA's list of data-level exemptions is fairly standard, including data processed in accordance with a variety of federal laws, such as the Health Insurance Portability and Accountability Act, federal research laws, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Driver's Privacy Protection Act and the Farm Credit Act, among others.

WHAT OBLIGATIONS ARE IMPOSED?

Controllers under MCDPA are subject to a number of obligations, including requirements to:

1. Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed and disclosed to the consumer;
2. Avoid processing personal data for secondary reasons (purposes that are neither reasonably necessary to nor compatible with the initial disclosed purposes) without the consumer's prior consent;
3. Establish, implement and maintain reasonable administrative, technical and physical data security practices (to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue);

4. Not collect, process or share sensitive data except where strictly necessary to provide or maintain a specific consumer-requested product or service;
5. Not process personal data in violation of laws that prohibit unlawful discrimination against consumers, and refrain from discriminating against consumers that exercise their rights;
6. Not process personal data for the purposes of targeted advertising or sell personal data if the controller knows that the consumer is between 13 and 16 years old;
7. Provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes the disclosures now common under state consumer privacy laws. Thankfully, MCDPA expressly states that a Minnesota-specific privacy notice or section of a privacy policy is *not* required where the body of the privacy policy otherwise includes the required disclosures; and
8. Document and maintain a description of the policies and procedures developed to comply with the requirements of MCDPA. Those documents must (i) include the name and contact information for the individual with responsibility for the policies and (ii) include a description of policies and procedures developed to implement different aspects of MCDPA including, for example, data minimization principles.

Of all these requirements, the last is a twist on other state laws. While most companies have likely already adopted some policies to implement other state privacy laws, companies will need to check those polices – or draft new ones – to ensure that they address the requirements of MCDPA.

WHAT CONSUMER RIGHTS ARE CREATED BY MCDPA?

MCDPA provides Minnesota consumers with consumer rights that should look familiar, with one notable exception relating to profiling:

1. The right to confirm whether or not the controller is processing the consumer's personal data and to access that data, if being processed;
2. The right to correct personal data, taking into account the nature of the data and the purposes of the processing of that data;
3. The right to require the controller to delete personal data concerning the consumer, unless required by law to retain the data;
4. The right to data portability when data processing is done through automated means;
5. Opt-out rights for targeted advertising, the sale of personal data and profiling, where profiling is being performed by automated means that produce legal or similarly significant effects concerning a consumer;
6. Where a consumer's personal data is profiled to advance decisions that produce legal effects or similarly significant effects (*e.g.*, housing, lending, financial, education), a right to request 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. Where the profiling was performed on incorrect data, the consumer has the right to request a correction of the information and a reevaluation of the profile;
7. A right to obtain a list of specific third parties to which a company has disclosed the consumer's personal information; and
8. The right to appeal rights requests that have not been fulfilled.

SENSITIVE DATA

MCDPA has a list of sensitive data that generally tracks with other state consumer privacy laws:

- Racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status;
- The processing of biometric or genetic information for the purpose of unique identification;
- Personal data of a known child (under 13); or
- Specific geolocation data.

The twist here is in the definition of "specific geolocation data." Whereas other state laws define that or similar terms as within a radius of a certain number of feet, under MCDPA, specific geolocation data includes (i) GPS-level latitude and longitude or (ii) other mechanisms, that directly identify the geographic coordinates of a consumer or device linked to a consumer with an accuracy of more than three decimal degrees of latitude and longitude or the equivalent in an alternative geographic coordinate system or (iii) a street address derived from either set of coordinates in (i) or (ii).

RESPONSE TO CONSUMER REQUESTS

Following the same framework as most states, under MCDPA, controllers must respond to a data subject request within 45 days after receipt, with a 45-day extension available as reasonably necessary. If denied, the controller must provide a method to appeal the denial of a request and make the process conspicuously available. A decision on the appeal must be provided within 45 days of receipt of the consumer's appeal, which can be extended by 60 additional days. If an appeal is denied, the decision must include a method for the consumer to submit a complaint with the Minnesota attorney general.

DATA PROTECTION ASSESSMENTS

MCDPA also requires controllers to conduct "data privacy and protection assessment[s]" for:

1. Processing personal data for targeted advertising;
2. Selling personal data;
3. Processing sensitive data;
4. Processing involving personal data that presents a heightened risk of harm to consumers (an undefined phrase in MCDPA); and
5. Processing personal data for purposes of profiling, where the profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment; (ii) financial, physical or reputational injury; (iii) a physical or other intrusion on the private affairs of a consumer; or (iv) other substantial injury to consumers.

The assessments must identify and compare the processing activity's benefits that may flow to all parties and potential risks to consumer rights. Like other state privacy laws, MCDPA allows impact assessments performed for other state privacy laws to satisfy its assessment requirements.

WHEN DOES MCDPA TAKE EFFECT?

Assuming it is signed into law, MCDPA will go into effect on July 31, 2025.

***

The plethora of unique state privacy laws is becoming more challenging as each new version is introduced. In addition to implementing comprehensive privacy programs, organizations need to ensure they are reviewing applicability and updating internal policies and procedures as needed to

maintain compliance.

National Law Review, Volume XIV, Number 145