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

Minnesota's Consumer Privacy Law Takes Aim at Profiling and Takes Effect Soon

Article By:

Cynthia J. Larose

Michael B. Katz

Rebecca Horton

It's the season of lists and next on ours: Minnesota! This state joined 18 others to enact comprehensive data privacy legislation in recent years. To avoid being on the "naughty" list, make sure to review your compliance program!

On May 19, 2024, Minnesota Governor Tim Walz (D) signed into law the Minnesota Consumer Data Privacy Act ("MNCDPA"), which will take effect on July 31, 2025. While the MNCDPA's framework is similar to many other state privacy laws already in effect, the law also includes notable provisions for small businesses and broader consumer rights around profiling. The following article explains what businesses are covered by the law and highlights key provisions of the MNCDPA.

To Whom Does the Minnesota Consumer Data Privacy Act Apply?

The Minnesota Consumer Data Privacy Act applies to entities that:

- conduct business in Minnesota or produce products or services that are targeted to residents of Minnesota; *and* during a single calendar year, satisfy one of the following criteria:
    1. control or process personal data of at least 100,000 consumers, not including personal data controlled or processed solely for the purpose of completing a payment transaction; *or*
    2. control or process personal data of at least 25,000 Minnesota consumers and derive over twenty-five percent (25%) of their annual gross revenue from the sale of personal data.

Like most other states, the MNCDPA defines a "consumer" as an individual who is a resident of Minnesota and acting only in an individual or household context. **This definition specifically excludes individuals acting in a commercial or employment context.**

Similarly to many other consumer privacy laws, the first prong of the MNCDPA expressly excludes

entities that control or process data for the sole purpose of completing payment transactions.

Finally, the law also applies to entities acting as "technology providers" under Minnesota Statute 13.32, which covers any persons who contract with public educational institutions to provide school-issued devices to students and create, receive, or maintain educational data. This is a notable effort on the part of Minnesota lawmakers to impose this law and its requirements on any business – big or small - providing technology to public schools and should be of key importance to ed tech providers.

Exemptions

The MNCDPA contains a number of categorical exemptions that are in line with many other state privacy laws. The law exempts government entities, federally recognized Indian tribes, state or federally chartered banks and credit unions, insurance companies, and nonprofits established to detect and prevent insurance fraud. **Minnesota is one of only a few states to exempt small businesses, as defined by the U.S. Small Business Administration; however, the law makes clear that such small businesses are prohibited from selling a consumer's sensitive data without prior consent (and are subject to enforcement under the MNCDPA for any violation of this restriction)**.

Additionally, the MNCDPA exempts certain types of data such as health records, protected health information ("PHI") under HIPAA, data for public health activities and purposes under HIPAA, consumer credit-reporting data, and information regulated by the Gramm-Leach-Bliley Act, the Family Educational Rights and Privacy Act, the Driver's Privacy Protection Act, the Farm Credit Act, the Airline Deregulation Act, and the Fair Credit Reporting Act. Note that these exemptions relate to the data and not to the entity, therefore, some personal data collected or processed by entities regulated by the various federal statutes could be required to comply with the MNCDPA as it relates to other types of personal data. The MNCDPA also exempts data processed or maintained for the purposes of job applications or employment, administering benefits, or collecting emergency contact information.

In contrast to some other states, the MNCDPA does not exempt higher educational institutions (though some will not be required to comply with its requirements until 2029). Moreover, the law contains only a narrow exemption for nonprofit organizations that have been established only for the purposes of detecting and preventing fraudulent acts of insurance fraud. **Many nonprofits may thus find themselves subject to the provisions of this law and should be prepared to comply with the MNCDPA**.

Consumer Rights

Minnesota consumers have the following rights under the MNCDPA:

- Right to confirm whether or not their personal data is being processed (unless access would require the business to reveal a trade secret);
- Right to access the categories of personal data being processed (again, unless access would require the business to reveal a trade secret);
- Right to correct inaccuracies in their personal data;
- Right to deletion of their personal data;
- Right to obtain a copy of their personal data;
- Right to obtain a list of specific third parties that have received their personal data from an entity; or, in the case that the entity does not have this information, a list of specific third

parties that have received *any* consumer personal data from the entity; and
- Right to opt-out of the processing of their personal data for purposes of:
    - (i) targeted advertising,
    - (ii) the sale of personal data, or
    - (iii) profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.

Importantly, the MNCDPA includes additional unique rights specific to profiling. If a consumer's personal data has been profiled in a way that produces legal or similarly significant effects, consumers have the following rights:

- Right to question the result of the profiling;
- Right to be informed of the reason for which the profiling resulted in the outcome;
- If feasible, the right to be informed of what actions they could have taken to produce a different decision;
- Right to review their personal data used in the profile; and
- If the personal data used in the profiling was incorrect, the right to correct the data and profiling decision.

Consumers may exercise their rights under the MNCDPA at any time by submitting a request to an entity specifying which rights they wish to exercise. Parents and legal guardians of children under thirteen (13) years of age may exercise such rights on their children's behalf.

Business Obligations to Consumers

The MNCDPA requires covered entities to:

- Provide at least one reliable means for consumers to submit a request to exercise their consumer rights;
- Respond to consumer requests within 45 days of receipt of such request (which may be extended an additional 45 days when reasonably necessary, depending on number and complexity of requests). If an entity receives an extension, it must notify the consumer of the extension and reason for the delay;
- If the business declines to act on the consumer's request, it must inform the consumer and provide instructions on how to appeal the decision that are conspicuously available and similar to the process for submitting consumer rights requests; and
- Within 45 days of receipt of a request for appeal, the business must inform the consumer of any action or inaction in response to the appeal, as well as a written explanation of reasoning supporting the decision and prominent information about how to file a complaint with the Office of the Attorney General. The response period may be extended by up to 60 days, where reasonably necessary.

Privacy Notices to Consumers

Covered entities must provide consumers with a "reasonably accessible, clear and meaningful" privacy notice that includes at a minimum the following:

- the categories of personal data that the business processes;
- the purposes for processing the personal data;
- an explanation of consumers' rights and how and where they can exercise such rights or

appeal an action;
- the categories of personal data that a business shares with third parties;
- the categories of third parties with which the business shares personal data;
- the business' contact information (including an active e-mail address or other online mechanism that the consumer may use to contact the business);
- a description of the business's retention policies for personal data;
- the date on which the business' privacy notice was last updated; and
- a conspicuous hyperlink to the privacy notice posted on the business' website, using the word "privacy" on the home page or mobile application's store page.

Note that businesses must provide reasonable notice to consumers of any material change to their privacy notice, taking into account available technology and the nature of the consumer relationship. In addition, businesses must provide a reasonable opportunity for those consumers to withdraw consent following the change.

Other Business Obligations

<u>THE DOs - Covered entities must:</u>

- Limit the processing of personal data to only the data that is "adequate, relevant, and reasonably necessary" to serve the purposes for which the data is collected and processed;
- Establish, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the confidentiality, integrity, and security of the personal data, including an inventory of the data that must be managed to exercise their obligations;
- Clearly and conspicuously disclose if the business sells consumers' personal data to third parties or engages in targeted advertising;
- Provide consumers with a conspicuous opportunity to opt out from the sale of their personal data to third parties or engaging in targeted advertising;
- Provide an effective mechanism for consumers to revoke their consent, which should be as easy to use as the mechanism for giving consent;
- Document and maintain a description of its policies and procedures it has adopted to comply with the MNCDPA, including the name and contact information of the business' Chief Privacy Officer or other individual charged with compliance;
- Conduct a data protection impact assessment for certain types of data use, including:
    - targeted advertising,
    - processing sensitive data,
    - selling personal data,
    - processing data for purposes of profiling, where profiling presents a reasonable risk of unfair or deceptive treatment of consumers, injury, intrusion upon privacy, or other substantial harm to consumers, and
    - any processing activities involving personal data with a heightened risk of harm to consumers.

<u>THE DON'Ts - Covered entities must not:</u>

- Process consumers' sensitive data without presenting the consumer with clear notice and an opportunity to opt out of such processing; or if the consumer is a child, without first obtaining consent from the child's parent or lawful guardian;
    - Sensitive data is defined as personal data that reveals racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship status, or

immigration status, genetic or biometric data, personal data of a known child, or precise geolocation data
- Prevent the retention of personal data that is no longer relevant or reasonably necessary for the purposes it was collected and processed;
- Process personal data in violation of state and federal laws that prohibit unlawful discrimination against a consumer; and
- Discriminate against consumers who exercise any rights under the MNCDPA.

Impact on Vendors and Data Processors

Processors such as vendors to covered businesses most often will have direct obligations under the MNCDPA, such as:

- adhering to instructions from the covered entity;
- assisting the covered entity with its own compliance obligations; and
- providing necessary information to enable the covered entity to conduct and document data protection impact assessments.

A processor must enter into contracts with covered businesses that govern how it processes personal data on the covered businesses' behalf. The MNCDPA prescribes the following requirements that must be included in data processing agreements between the parties:

- instructions for processing personal data;
- the nature and purpose of processing;
- the type of data subject to processing;
- the duration of processing; and
- the rights and duties of both parties.

Furthermore, the contract must require the processor to do the following:

- ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
- at the business' direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;
- upon the reasonable request of the business, make available all information in its possession necessary to demonstrate the sub processor's compliance with the obligations of the MNCDPA;
- after providing the business an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and
- allow, and cooperate with, reasonable assessments by the business or the business' designated assessor, or the subprocessor may arrange for a qualified and independent assessor to conduct an assessment of the subprocessor's policies and technical and organizational measures in support of the obligations under the MNCDPA. This assessment must be available to the business upon request.

De-identified and Pseudonymous Data

The MNCDPA defines "deidentified data" as data that cannot reasonably be linked to an identified or identifiable individual, and such data is expressly excluded from the definition of "personal data." As

with other state privacy laws, the MNCDPA requires businesses to take reasonable measures to ensure that such data cannot be associated with an individual and contractually require recipients of deidentified data to comply with such provisions. The MNCDPA, along with a few other states such as Virginia and Connecticut, also requires entities to "publicly commit" to only process data in a deidentified fashion and not attempt to reidentify such data.

Further, the MNCDPA defines "pseudonymous data" as "personal data that cannot be attributed to a specific natural person without the use of additional information." In cases where entities can show that any additional information necessary to identify a consumer is (i) kept separately and (ii) subject to effective technical and organizational measures that prevent the business from accessing such information, then a consumer's rights to access, delete, and opt-out will not be available for such pseudonymous data.

In general, the MNCDPA requires businesses that use deidentified or pseudonymous data to exercise reasonable oversight to ensure compliance with contractual commitments with third parties dealing with such data. Businesses should also take prompt and reasonable actions to address any breaches of these provisions.

Enforcement

As with many state consumer privacy laws, the MNCDPA does **not** provide consumers with a private right of action. The Minnesota Attorney General will have exclusive authority to enforce the MNCDPA.

The law also provides for a thirty-day cure period where, prior to bringing an enforcement action, the Attorney General will provide a violating entity with a "warning letter" identifying the specific provisions of the MNCDPA that have allegedly been violated. Entities will have thirty days to cure alleged violations or else face enforcement action. **Readers should note that Minnesota will no longer offer such "cure periods" after January 31, 2026**.

Fines and Penalties

If violations are left uncured, the Minnesota Attorney General may initiate enforcement actions against entities to recover up to $7,500 in civil penalties per violation. Violators will also be subject to an injunction and part or all of the Attorney General's litigation expenses.

Index

Here are links to our articles covering all other states that have enacted consumer privacy laws:

Iowa

Maryland

Montana

Nebraska

New Hampshire

New Jersey

Oregon

Rhode Island

Tennessee

Texas

Utah

Virginia

National Law Review, Volume XIV, Number 365