Blogs
June 07, 2024
Minnesota's Unique Spin on Consumer Data Privacy

Minnesota's governor signed the Minnesota Consumer Data Privacy Act (MNCDPA or the Act) into law at the end of May, making Minnesota the 18th state to enact a comprehensive consumer privacy law.

The MNCDPA will take effect for most covered entities on July 31, 2025. The law provides a 30-day cure period, which will sunset on January 31, 2026, six months after the Act's effective date. Entities that violate the Act are subject to injunction and civil penalties of up to $7,500 per violation. Like most other state privacy laws, the MNCDPA does not include a private right of action and will be enforced solely by the attorney general.

While the MNCDPA shares many similarities with other state consumer privacy laws, it also introduces several unique elements that set the Act apart. Here we delve into the distinctive aspects of the MNCDPA:

1. **The Right to Question the Results of Profiling**

Like many other state privacy laws, the MNCDPA requires that covered entities[1] provide consumers the ability to opt out of having their personal data processed for the purpose of "profiling" in furtherance of automated decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.

In addition to that more common opt-out right, Minnesota provides consumers with the unique right to question the result of the profiling (which is defined broadly as any form of automated processing of personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements). Specifically, under the MNCDPA, if a consumer's personal data is profiled in furtherance of decisions that produce legal effects or "similarly significant effects" concerning a consumer, the consumer has the right to (1) 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; (2) review the consumer's personal data used in the profiling; and (3) if the decision is determined to have been based upon inaccurate personal data, have the data corrected and the profiling decision reevaluated based upon the corrected data.

While the opt-out right only applies to profiling that leads to "*automated* decisions" with legal or similarly significant effects, the right to question the result of profiling applies to any decisions with such effects.

2. **Heightened Data Security Requirements**

Like the majority of states, the MNCDPA requires controllers to establish, implement, and maintain reasonable data security practices to protect the confidentiality, integrity, and accessibility of personal data. Minnesota goes one step further by requiring covered entities to create and maintain "an inventory of data that? must be managed to exercise these responsibilities"—commonly referred to as a data inventory or data mapping. This is the first state privacy law to impose such a requirement, although data mapping has long been required under the European Union's General Data Protection Regulation (GDPR) and viewed as a best practice for addressing compliance requirements under the other state privacy laws. The Act provides no specific definition or guidance as to what specific data must be inventoried.

The MNCDPA also requires controllers to document and maintain a description of the policies and procedures the controller has adopted to comply with the MNCDPA, including the name and contact information for the controller's chief privacy officer or other individual with primary responsibility for directing the policies and procedures. Again, this is the first time we see such a requirement under U.S. state privacy laws, but the concept mirrors the requirement to appoint a data protection officer under the GDPR and other international data protection laws.

3. **Protections for Teens**

Like many other state privacy laws, under the MNCDPA, the personal data of a "known child" is considered sensitive data, and entities are required to obtain consent from the child's parent or lawful guardian before processing the child's personal data. The Act is more explicit than other omnibus state consumer privacy laws in expressly prohibiting controllers from processing the personal data of consumers for the purpose of targeted advertising where the controller knows the consumer is between the ages of 13 and 16.

4. **Identification of Specific Third Parties Who Receive Personal Data**

Unlike most other state laws, the MNCDPA includes a right for consumers to request the identities of the specific third parties to whom their personal data has been disclosed or, if that information is unavailable, a list of specific third parties to whom the controller has disclosed *any* individual's personal data. The Oregon Consumer Privacy Act includes a similar provision.

5. **Addition of Nondiscrimination Protections**

State privacy laws typically prohibit controllers from processing personal data in violation of anti-discrimination laws. The MNCDPA goes a step further than most state privacy laws and explicitly requires that controllers shall not process personal data on the basis of a consumer's actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, lawful source of income, or disability in a manner that unlawfully discriminates against the consumer with respect to the offering or provision of: housing, employment, credit, or education; or the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation.

6. **Additional Requirements for Privacy Notices and Assessments**

The MNCDPA contains unique transparency obligations requiring that controllers include in their privacy notice a description of the controller's retention policies for personal data as well as the date the notice was last updated.

Implications for Businesses

While the MNCDPA is in many ways similar to other state privacy laws, there are some notable differences. As such, covered entities should review and update their data privacy practices to ensure they are complying with the new law by the time it goes into effect. Among other things, covered entities should:

- Update notices and procedures for responding to consumer rights requests, including the new right to question profiling, the requirement to disclose the names of the specific third-party recipients of a consumer's personal data, and additional disclosure requirements related to sensitive data;
- Maintain an accurate and complete data inventory and appoint a chief privacy officer;
- Prepare public-facing retention statements and/or policies;
- Assess targeted advertising practices to avoid tracking known children under the age of 16; and
- Train employees on data privacy obligations and consumer rights under the MNCDPA.

---

[1] Under the Act, covered entities are legal entities that conduct business in Minnesota or produce products or services that are targeted to residents of Minnesota and that satisfy one or more of the following thresholds: (1) during a calendar year, controls or processes personal data of 100,000 consumers or more, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) derives over 25 percent of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more. Like many other state consumer privacy laws, the Act exempts personal data covered by certain federal and state privacy laws and certain types of entities.

Authors

Explore more in

Privacy & Security State Consumer Privacy Laws