



Alerts

Q&A: How Businesses Must Comply with a New Minnesota State Privacy Law

June 13, 2024

Privacy, Cyber & AI Decoded

On May 24, 2024, Senate Bill 4757, containing a comprehensive Minnesota Consumer Data Privacy Act (MCDA), was signed into law by Minnesota Governor Tim Walz. It will take effect on **July 31, 2025**.

Who Does the MCDA Apply to?

Similarly to other state privacy laws, the MCDA applies to:

1. legal entities that conduct business in Minnesota, or
2. produce products or services that are targeted to Minnesota residents and that satisfy one or more of the following thresholds:
 - (a) during a calendar year, control or process personal data of 100,000 consumers or more, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
 - (b) derive over 25 percent of gross revenue from the sale of personal data and process or control the personal data of 25,000 consumers or more.

The MCDA also applies to technology providers who contract with a public educational agency or institution to provide a school-issued device for student use and create, receive, or maintain educational data pursuant to or incidental to a contract with a public educational agency or institution.

Does Your Business Fall Within an Exception?

The MCDA provides exemptions similar to what other states have exempted from coverage, including:

- information covered by the Health Insurance Portability and Accountability Act (HIPAA) or other specified health-related information by the MCDA;
- an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency;

Attorneys

Justyna H. Regan, Ph.D.

Service Areas

Privacy, Security & Artificial Intelligence



- personal data collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (GLB) or Driver's Privacy Protection Act (DPPA); and
- employment-related data.

The MCDA also excludes certain types of businesses, such as:

- insurance companies,
- not-for-profits,
- small businesses-as defined by the Small Business Administration (SBA),
- or air carriers.

Which Key Provisions Should My Business Look Out For?

1. Requirement of a Written Agreement Between a Controller and a Processor

The MCDA, like the California Consumer Privacy Act (CCPA), requires an agreement to be reached between the controller and the processor that sets out processing instructions that are binding to the processor.

The agreement must also address other matters listed by the MCDA, such as the processor's obligation to delete or return all personal data at the controller's choice and allowing and contributing to reasonable assessments and inspections by the controller or the controller's designated assessor.

2. Consumer Rights

The MCDA provides a list of consumer rights that include:

- the right to confirm whether a controller is processing personal data concerning the consumer and access the categories of personal data the controller is processing, as well as the right to correct inaccurate personal data;
- the right to delete personal data; the right to obtain personal data concerning the consumer, which the consumer previously provided to the controller (only applicable to processing carried out by automated means);
- the right to question the result of the profiling; and
- the right to obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data.

The MCDA specifies that the controller shall respond to the consumer's request without undue delay and within 45 days of receipt at the latest. It is worth noting that no waiver of consumer rights is deemed enforceable under the MCDA.

3. The Right to Opt Out

The MCDA also equips consumers with the right to opt out of the processing of personal data for purposes of targeted advertising, selling personal data, or profiling in furtherance of automated decisions that produce legal effects concerning a consumer.

Such right shall be facilitated through an opt-out preference signal sent, with the consumer's consent, by a platform, technology, or mechanism to the controller indicating the consumer's intent to opt out of any processing or sale.

5. Putting an Appeal Process in Place

According to the MCDA, the controller should establish and make available an internal process whereby a consumer may appeal a refusal to take action on a request to exercise any of the consumer rights.



Privacy Notice

The controller is obligated to provide a privacy notice that shall:

- specify the categories of personal data processed and the purpose of such processing;
- explain consumer rights, category of data sold, and entities such data is sold to; and
- explain the retention policy and provide a way to opt out of the sale of personal data and its processing for targeted advertising or profiling.

Every time such a Minnesota privacy notice is amended, consumers affected by the change must be notified so that they can withdraw their consent.

Data Privacy Protection Assessment

When sensitive data is processed, personal data is sold, processed for purposes of targeted advertisement, profiling, or whenever processing involves personal data that presents a heightened risk of harm to consumers, the controller is obligated to conduct and document a data privacy protection assessment.

How and When is the Act Enforced?

The MCDA will be enforced by the Minnesota Attorney General starting **July 31, 2025**. It does not provide for a private right of action.