Jul 31, 2025

Categories:

Publications

Authors:

Mason C. Clutter

Caleb S. Long

Minnesota Consumer Data Privacy Act: What Businesses Need to Know

The Minnesota Consumer Data Privacy Act went into effect July 31, 2025. Modeled after many states' existing comprehensive consumer privacy laws, the Minnesota law includes some unique features related to consumers' rights to question profiling-related decisions, the "selling" of personal data for individuals between the ages of 13 and 16, and a requirement to document policies and procedures designed to comply with the law, among others.

This article breaks down key aspects of the Minnesota Consumer Data Privacy Act to help you assess whether your business may be subject to the law and, if so, what it requires.

Effective Date

- July 31, 2025 (except for application to certain post-secondary institutions for which the law is effective July 31, 2029).

Who Is Impacted?

- The law applies to businesses that do business in Minnesota or produce products or services targeted to residents of Minnesota, and that:
    - Control or process the personal data of at least 100,000 Minnesota residents in a calendar year (excluding information solely processed for the purpose of completing a payment transaction); or
    - Control or process the personal data of at least 25,000 Minnesota residents and derive 25% or more of their gross revenue from the "sale" of personal information.

- Notably, Minnesota is one of a few states that exempt small businesses, as defined by the U.S. Small Business Administration; however, small businesses must obtain consent before "selling" a consumer's sensitive personal information.
- "Personal data" is defined as any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include deidentified data or publicly available information.

Frost Brown Todd ATTORNEYS

- In this context, "publicly available information" means information that (1) is lawfully made available from federal, state, or local government records or widely distributed media, or (2) a controller has a reasonable basis to believe has lawfully been made available to the general public.

- "Controller" is defined as the natural or legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "Processor" is defined as a natural or legal person who processes personal data on behalf of a controller.
- "Consumer" is defined as a natural person who is a Minnesota resident acting only in an individual or household context. Consumer does not include a natural person acting in a commercial or employment context.
- "Sale" is defined as the exchange of personal data for monetary or other valuable consideration by the controller to a third party.

A Few Key Exemptions

Exemptions under the Minnesota Consumer Data Privacy Act include, but are not limited to, the following:

- Information governed by the Health Insurance Portability and Accountability Act of 1996, the Gramm-Leach-Bliley Act, and the Family Education Rights and Privacy Act.
- Nonprofit organizations established to detect and prevent fraudulent acts in connection with insurance.
- Use of personal information for certain specific purposes, such as compliance with law, preventing fraud or injury, and defending legal claims.

What to Know if You Are Covered by the Act

- **Rights of Minnesota consumers:** Minnesota residents have the following rights regarding their personal information:
  - Confirm whether a controller is processing the consumer's personal data;
  - Access the consumer's personal data;

- Correct personal data the consumer previously provided to a covered business;
- Delete personal data (information from or about the consumer);
- Obtain a copy of the personal data the consumer previously provided to a covered business (i.e., "data portability"), though the business must not provide sensitive personal information to the requester, just the fact of collection of sensitive data elements (e.g., social security number, driver's license number);
- Opt-out of the sale of the consumer's personal information used for targeted advertising, or "profiling in furtherance of automated decisions that produce legal effects concerning the consumer or similarly significant effects concerning the consumer";
- Obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data;
- Appeal a denial of a consumer's rights request and file a complaint with the Minnesota Attorney General if the appeal is also denied;
- Be free from discrimination for exercising a consumer right.

Additionally, Minnesota provides the following unique consumer rights for individuals subject to "profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer":

-
  - Right to question the result of profiling;
  - Right to be informed of the reason that the profiling resulted in the decision;
  - Right to, if feasible, be informed of what actions the consumer might have taken to secure a different decision in the future; and
  - Right to review the consumer's personal data used in the profiling and, if the decision was based on inaccurate personal data, "to have the data corrected and the profiling decision reevaluated based upon the corrected data."

- **Data minimization standard:** Covered businesses must limit their collection of personal information to what is "adequate, relevant, and reasonably necessary" for the purposes for which they process the personal information, as disclosed to consumers. Additionally, covered businesses

may not process personal information for purposes that are not "reasonably necessary to or compatible with" the disclosed purposes for processing unless the business first obtains the consumer's consent.

- **Data security and data inventory:** Covered businesses must maintain "reasonable administrative, technical, and physical data security practices" proportionate to the nature and volume of the personal information collected. Additionally, the Minnesota law includes a unique requirement to create and maintain a data inventory reflecting the personal information that must be managed to comply with the security requirements.
- **Sensitive personal information:** Covered businesses must obtain consent from the data subject (or, in the case of a known child under the age of 13, in accordance with the Children's Online Privacy Protection Act) before processing "sensitive personal information."
    - "Sensitive Personal Information" includes but is not limited to:
        - Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status;
        - Biometric data or genetic information for the purpose of uniquely identifying an individual;
        - Personal data of a known child (under the age of 13); and
        - Specific geological data.

- **Privacy policy:** Covered businesses must provide a privacy notice that contains specified elements, including:
    - Categories of personal data processed;
    - Purposes for which the categories of personal data are processed;
    - Rights consumers are entitled to and how they may exercise such rights, including how to appeal a denial of a request to exercise such rights;
    - Categories of personal data that the controller sells to or shares with third parties;
    - Categories of third parties with whom the covered business sells or shares personal data;

- Description of the controller's retention policies for personal data; and
- Date the privacy notice was last updated.

In addition, the policy must be (1) provided in each language in which the covered entity provides a product or service and (2) reasonably accessible and usable to individuals with disabilities.

The Minnesota law, like the California Consumer Privacy Act, requires that notice be provided outside of the privacy policy about a consumer's right to opt-out of the sale, processing, or profiling "in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer." There is no one way to comply with this requirement. The statute provides an example of "an Internet hyperlink clearly labeled 'Your Opt-Out Rights' or 'Your Privacy Rights' that directly effectuates the opt-out request or takes consumers to a webpage where the consumer can make the opt-out request."

Finally, covered entities must provide consumers with notice of a material change to the business's privacy policy or procedures and give them a reasonable opportunity to "withdraw consent to any further materially different collection, processing, or transfer of previously collected personal data under the changed policy."

- **Individuals 13 to 16 years old:** If a covered business knows that a consumer is between the ages of 13 and 16, the business must not process their personal data for purposes of targeted advertising, or sell their personal data, without their consent. While the processing of personal data of consumers under 13 is governed by the Children's Online Privacy Protection Act, Minnesota provides additional protection for consumers between 13 and 16 years old.
- **Universal opt-out mechanisms:** Minnesota joins the list of states that permit consumers to—and therefore requires covered entities to honor—opt-out preference signal (such as Global Privacy Control), effectively opting the consumer out of processing of their personal data for the purposes of targeted advertising or sale.
- **Data privacy protection assessments:** Like many states, Minnesota requires that covered businesses perform "data privacy and protection assessments" for specified activities, including the use of personal

information for targeted advertising, sale, profiling, and processing activities that "present a heightened risk of harm to consumers."

Data privacy and protection assessments must, in part, identify and assess (1) the potential risks and benefits of the proposed processing activities to the consumer, other stakeholders, and the public and (2) any appropriate mitigation measures employed by the business to mitigate the identified potential risks.

- **Privacy policies and procedures:** Another unique requirement under the Minnesota Consumer Data Privacy Act is that covered entities are required to document and maintain a copy of the policies and procedures adopted to comply with the law, including, as applicable, the contact responsible for implementing the respective policies and procedures, how the business will comply with data subject access requests, required security practices (including the above-mentioned data inventory), and retention policies and practices.

Enforcement

- **No private right of action:** The Minnesota attorney general has exclusive authority to enforce this regulation. There is no private right of action for consumers to bring suit under the law.
- **Temporary cure period:** Through January 31, 2026, the attorney general must provide a covered entity with a warning letter identifying the specific provisions of the regulation the attorney general alleges have or are being violated. The entity then has 30 days to cure the violation(s). Thereafter, the attorney general may bring a civil action against the business.
- **Penalties and available remedies:**
  - Injunction
  - Up to $7,500 for each violation, plus the reasonable value of all or part of the state's litigation expenses.

What to Do Now?

This is just a snapshot of some of the key features of the Minnesota Consumer Data Privacy Act. If you think you may be covered by this or other U.S. state privacy laws, please contact your attorney to ensure your data privacy and security practices appropriately comply with the law. While compliance can be challenging,

it also presents an opportunity to determine how to comply in a manner that is consistent with the way in which you do business and engage with consumers, setting yourself apart from others in the marketplace.

At Frost Brown Todd, we view compliance as an opportunity to not only comply with the law but to build and maintain trust with your customers while saving time and resources along the way. If you have questions or need immediate assistance, please contact the authors or any attorney with Frost Brown Todd's Data Security and Privacy team.

Frost Brown Todd
ATTORNEYS