

The MNDPA (effective July 31, 2025) governs certain entities that control (“controllers”) or process (“processors”) and, as applicable, sell, the personal data of Minnesota residents, other than in the employment or business-to-business contexts (“consumers”). It also grants Minnesota residents certain rights with respect to their personal data.

Applicability

The MNDPA applies to legal entities that conduct business in Minnesota or produce products or services that are targeted to consumers, and who during the preceding calendar year either:

- Controlled or processed the personal data of at least **100,000** consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction, or
- Derived more than **25%** of their gross revenue from the sale of personal data and controlled or processed the personal data of at least **25,000** consumers.

Practical Application for Businesses

Consumer Rights:

- (1) **Right to Access:** the right to confirm whether a controller is processing personal data, access such data, and obtain a list of third parties to which personal data was disclosed.
- (2) **Right to Correct:** the right to correct inaccuracies in the consumer’s personal data (taking into account the nature of the personal data and the purposes of processing the data).
- (3) **Right to Delete:** the right to delete personal data concerning the consumer.
- (4) **Right to Data Portability:** the right to obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance, where the processing is carried out by automated means.
- (5) **Right to Opt Out:** the right to opt out of the processing of personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of automated decisions that significantly affect a consumer.
- (6) **Right to Question:** the right to question profiling in furtherance of decisions that significantly affect a consumer, including to question the results of profiling, correct inaccurate data, and have the profiling decision reevaluated.

Controller Obligations:

- Publish a privacy notice that contains requisite details, notify consumers of material changes thereto, and provide an opportunity to consumers to withdraw consent from any materially-affected collection or processing practices.
- Obtain consent to collect sensitive data and process sensitive data of consumers under **13** per COPPA.
- Provide consumers with sufficient methods to exercise their rights, including universal opt-out mechanisms.
- Act on consumer requests within **45 days**; provide notice of extensions and the appeals process as necessary.
- Enter into binding data processing agreements with requisite limitations for third-party processors.
- Conduct and document a data protection assessment for each processing activity that poses a “heightened risk of harm” to the consumer (e.g., selling personal data, processing sensitive data, or targeted advertising or profiling with certain foreseeable risks).

Recommendations for Controllers:

- Regularly update data maps to detail personal data collection, including sensitive data and targeted advertising.
- Train employees how to handle consumer inquiries and requests.
- Maintain clear and executable data retention policies and procedures.

Penalties:

- The Minnesota Attorney General has exclusive enforcement authority. A violation of the MCDPA could result in civil penalties up to **\$7,500 per violation**.
- From July 1, 2025 until January 31, 2026, there is a 30-day cure period to correct violations.