Articles + Publications | June 4, 2024

Minnesota Enacts the Latest State Privacy Law – HF 4757 / SF 4782

WRITTEN BY

Kim Phan | Laura Hamady | Alexandria Pritchett

On May 24, Minnesota Governor Tim Walz (D) signed the Minnesota Consumer Data Privacy Act (MCDPA) into law. The MCDPA largely aligns with previous state consumer privacy laws, but it introduces some significant and novel variations. These distinctions include requiring controllers to maintain a data inventory, to document and maintain a description of policies and procedures adopted to comply with the MCDPA's provisions, and to allow consumers to assign their rights to an authorized agent by way of an "Internet link or a browser setting." With this enactment, Minnesota becomes the 18th U.S. state to enact a comprehensive privacy law. The MCDPA will take effect on July 31, 2025, and will be enforceable by the state attorney general (AG), but unlike some other states, it does not confer any rulemaking authority to the AG.

Applicability

The MCDPA applies to "all legal entities that conduct business in Minnesota or produce products or services that are targeted to residents of Minnesota," if the entity satisfies any one of the following thresholds:

1. Controls or processes personal data of 100,000 consumers or more during a calendar year, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
2. Derives more than 25% of gross revenue from the sale of personal data and processes, or controls personal data of 25,000 consumers or more.

Exemptions

The MCDPA provides several exemptions, including both entity-level exemptions and data-level exemptions.

The entity-level exemptions include government entities, certain financial entities such as banks and insurance companies, small businesses, airlines, and federally recognized Native American tribes. Interestingly, nonprofits are *not* exempt unless they were "established to detect and prevent fraudulent acts in connection with insurance." Additionally, the MCDPA excludes small businesses as defined by the U.S. Small Business Administration. This approach is similar to those found in Texas and Nebraska. Despite the exemption, the MCDPA includes a prohibition against small businesses selling a consumer's sensitive data without prior consent, regardless of the number of consumers whose data they process.

Categories of data-level exemptions include a variety of federal laws, such as the Health Insurance Portability and Accountability Act, federal research laws, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Driver's

Privacy Protection Act, Family Educational Rights and Privacy Act, and the Farm Credit Act, among others.

Minnesota also includes an employee and business-level exemption that exempts data collected or maintained "in the course of an individual acting as a job applicant to or an employee, owner, director, officer, medical staff member or contract of a business."

The MCDPA devotes an entire section to whether its requirements should apply to pseudonymous or deidentified data, including the types of technical and organizational controls that would need to be implemented to benefit from this exemption. Specifically, the statute defines pseudonymous data as "personal data that cannot be attributed to a specific natural person without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." The MCDPA further outlines certain obligations for controllers processing de-identified data that seem less stringent than for controllers processing identified data. For example, a controller that uses pseudonymous data only has to "exercise *reasonable* oversight to monitor compliance," whereas a controller of personal data generally must "establish, implement, and maintain reasonable administrative, technical, and physical data security practices" to protect the data.

Consumer Rights

The MCDPA provides for the typical set of consumers rights similar to other state privacy laws, including the right to access, right to correct, right to delete, right to portability, and right to opt out of processing (only for targeted advertising, sales, or profiling).

With regards to profiling, the MCDPA provides additional consumer rights. If a consumer's personal data is profiled to make decisions that produce legal effects concerning a consumer or similarly significant effects, the consumer has the right to question the result of the profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions they might have taken to secure a different decision and the actions they might take to secure a different decision in the future. The consumer has the right to review their personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data, considering the nature of the personal data and the purposes of the processing of the personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

The MCDPA varies from previous state privacy laws by also providing a right to obtain a specific list of third parties to which a controller has disclosed a consumer's personal data, rather than merely a description of the categories of such third parties. The MCDPA also requires honoring a universal opt-out mechanism for opting out of both targeted advertising and sales of personal data.

With regards to requests to delete, if a controller has obtained a consumer's personal data from a source other than directly from the consumer, for such personal data, the controller may comply with a consumer's request to delete their personal data by either: (1) retaining a record of the deletion request, retaining the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted, and not using the retained data for any other purpose; or (2) opting the consumer out of the processing of personal data for any purpose

except for the purposes exempted by the MCDPA.

Consumers will also be able to appeal any decisions made by a controller in response to a consumer request to exercise any of these rights. The MCDPA provides additional details about how controllers should respond to such appeals. A controller must provide a written explanation of the reasons for the controller's decision and clearly and prominently provide the consumer with information about how to file a complaint with the Office of the AG.

Controller and Processor Obligations

Controllers under MCDPA are subject to several obligations that are similar to those articulated under other state privacy laws. Some of the similarities include a controllers' obligation to limit the collection of personal data, avoid processing data for secondary reasons without consumer consent, enter into contracts between controllers and processors that contain specific statutory language, conduct and document data privacy and protection assessments for certain types of processing, and avoid collecting and processing sensitive data in a way that violates laws that prohibit unlawful discrimination of consumers.

Additionally, the following requirements are unique to the MCDPA:

1. Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes the disclosures now common under state consumer privacy laws. Unlike other state privacy laws, the MCDPA dictates that whenever a controller makes a material change to the controller's privacy notice or practices, they must notify consumers affected by the material change with respect to any prospectively collected personal data, and provide a reasonable opportunity for consumers to withdraw consent to any further materially different collection, processing, or transfer of previously collected personal data under the changed policy. The controller must take all reasonable electronic measures to provide such notification.

2. Like other state privacy laws, the MCDPA imposes an affirmative obligation to establish, implement, and maintain data security practices. However, the MCDPA is the first to require the maintenance of a data inventory as part of such data security practices.

3. Controllers must document and maintain a description of the policies and procedures developed to comply with the requirements of MCDPA. Those documents must (i) include the name and contact information for the individual with responsibility for the policies, and (ii) include a description of policies and procedures developed to implement different aspects of MCDPA including, for example, data minimization principles.

Practice Tips

To prepare for the MCDPA's potential enactment, companies should assess whether one of the novel controller obligations may apply to their business. Specifically, a company should assess whether they process identified vs. deidentified data, have a robust privacy notice, and how notice of any future privacy notice changes will be communicated to consumers. Companies should also proactively document an inventory of data, as well as develop comprehensive policies and procedures for complying with the MCDPA pursuant to the laws' controller obligations.

Additionally, companies should be aware of certain exemptions and nuances in the MCDPA that may pose an

increased risk for litigation and liability. For example, the MCDPA allows consumers to assign their rights to an authorized agent by way of an “Internet link or a browser setting,” which could result in an influx of requests by one entity on behalf of various consumers.

Lastly, the MCDPA provides for a 30-day right to cure provision whereby the AG must provide a controller or processor a warning letter that outlines the alleged violations. Companies should be prepared with a robust plan of action to cure any deficiencies identified within a 30-day timeframe. Notably, the 30-day right to cure provision is a sunset provision that ends in 2026.

Troutman Pepper will continue to monitor the MCDPA as well as all other data privacy law developments.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber