THOMPSON HINE

Privacy & Cybersecurity Update

May 2024

Minnesota Legislature Passes Consumer Privacy Law

On May 19, the Minnesota Legislature passed a broad omnibus bill that contained the Minnesota Consumer Data Privacy Act (MCDPA), which furnishes Minnesota residents with several data protection rights and requires covered businesses to comply with new data privacy and information security requirements. The MCDPA, however, does not create a private right of action and delegates enforcement authority to the Minnesota attorney general. Minnesota Governor Walz is expected to sign the omnibus bill into law, and if so, the bill will enter into force on July 31, 2025, for most covered businesses.

Scope of Applicability

The MCDPA generally applies to organizations that conduct business in Minnesota or produce products or services that are targeted to Minnesota residents and either (i) during a calendar year, controls or processes personal data of 100,000 consumers or more (which does not include personal data processing for payment transactions, *or* (ii) (a) derives over 25% of gross revenue from the sale of personal data *and* (b) processes or controls personal data of 25,000 consumers or more.

The law also notes that a "technology provider," as defined under Minnesota's education record law, must comply with both the education records law and the MCDPA, provided that a provider's obligations under the education record law take precedence if a conflict arises between the two.

The MCDPA includes several exemptions that are standard in data privacy frameworks, including exemptions for state and local governments, organizations governed by federal law (e.g., HIPAA, GLBA, FERPA), and certain insurance companies, small businesses (as defined by the United States Small Business Administration), a nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance, and air carriers subject to the federal Airline Deregulation Act, among others.

Key Terms

The MCDPA primarily regulates how data "controllers" and "processors" can collect and process a consumer's personal data. The term, "consumer," is defined as any Minnesota resident acting in an "individual or household context." The term generally excludes personal data concerning individuals acting in a commercial or an employment capacity, including "HR data" and personal data related to job applicants. It also does not include "deidentified data" or "publicly available information," each of which has its own definition under the law.

The MCDPA creates additional requirements when an entity processes "sensitive data," which is defined as a subset of personal data that means: (i) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status, (ii) the processing of biometric data or genetic information to uniquely identify an individual, (iii) the personal data of a known child, or (iv) specific geolocation data.

Consumer Privacy Rights and Appeals

As with other state privacy laws, the MCDPA grants consumers the rights to:

- Confirm whether a controller is processing personal data concerning the consumer and access the categories of personal data the controller is processing.
- Correct inaccurate personal data concerning the consumer, considering the nature of the personal data and the purposes of the processing of the personal data.
- Delete personal data concerning the consumer.
- Obtain personal data concerning the consumer, which they previously provided to the controller, in a portable and, to the extent technically feasible, readily usable format that allows them to transmit the data to another controller without hindrance, where the processing is carried out by automated means.
- Obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data. If the controller does not maintain the information in a format specific to the consumer, they may instead provide a list of specific third parties to whom they have disclosed any consumer personal data.

The MCDPA requires controllers to establish a process for receiving, processing, and responding to data privacy requests, including how to "authenticate" consumer requests and timelines for when responses must be furnished to consumers. The law also requires controllers to create a framework for how consumers can appeal a controller's decision on responding to a privacy request. Importantly, when informing a consumer of any action taken or not taken in response to an appeal, a controller must provide the consumer with 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 Attorney General." The controller must maintain records of all appeals and the controller's responses for at least 24 months.

Opt-Out Rights - Profiling

The MCDPA grants consumers the right to opt out of the processing of their personal data for profiling in furtherance of automated decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.

If a consumer's personal data is profiled in these circumstances, they also have the right (i) to question the result of the profiling, (ii) to be informed of the reason that the profiling resulted in the decision, and, (iii) 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. The consumer has the right to review the personal data used in their profiling. If the decision was based on inaccurate personal data, the consumer has the right, in some circumstances, to have the data corrected and to have the profiling decision reevaluated based on the corrected data.

Opt-Out Rights - Targeted Advertising and Sales

In addition to the aforementioned rights, the MCDPA grants consumers the right to opt out of processing their personal data for targeted advertising purposes and the sale of personal data.

The term "targeted advertising" means "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests." However, as with the definition of "sale of personal data," the definition of "targeted advertising" includes several exceptions within its meaning that are common across other U.S. state data protection laws.

The MCDPA's definition of the "sale of personal data" is like that found in other U.S. state data protection laws: "the exchange of personal data for monetary or other valuable consideration by the controller to a third party." However, several activities are excluded from its scope, such as:

- the disclosure of personal data to a processor (e.g., service provider),
- the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer,

- the disclosure or transfer of personal data to an affiliate of the controller,
- the disclosure of information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience,
- the disclosure or transfer of personal data to a third party as an asset that is part of a corporate restructuring or bankruptcy, or
- the exchange of personal data between the producer of a good or service and authorized agents of the producer who sell and service the goods and services to enable the cooperative provisioning of goods and services by both the producer and the producer's agents.

A consumer may designate another person as the consumer's authorized agent to exercise the consumer's right to opt out of the processing of the consumer's personal data for purposes of targeted advertising and sale and such designation may occur by way of, among other things, a technology, including, but not limited to, an internet link or a browser setting, browser extension, or global device setting, indicating the consumer's intent to opt out of the processing. A controller shall comply with an opt-out request received from an authorized agent if the controller can verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

Controller Obligations, Consent, and Small Businesses

A controller (i) must "limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data are processed, which must be disclosed to the consumer" and (ii) may not, unless an exception applies, "process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which the personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent."

Generally, a controller may *not* process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of personal data concerning a known child, without obtaining consent from the child's parent or lawful guardian. Further, a controller must "provide an effective mechanism for" individuals to revoke their consent, and this mechanism must "be at least as easy as the mechanism by which the consent was previously given." If a consumer's consent is revoked, then a controller must cease its data processing as soon as practicable, but not later than 15 days after receiving the request.

A controller may not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data, without the consumer's consent, under circumstances where the controller knows that the consumer is between the ages of 13 and 16.

Notwithstanding other exemptions within the law, the MCDPA provides that a small business that conducts business in Minnesota or produces products or services that are targeted to residents of Minnesota must not sell a consumer's sensitive data without the consumer's prior consent.

Privacy Notices

Under the MCDPA, a controller must provide consumers with a "reasonably accessible, clear, and meaningful privacy notice that includes" the following information:

- the categories of personal data processed by the controller and the purposes for which it is processed,
- an explanation of the consumer's data privacy rights (including appeals) and processes for exercising them,
- the categories of personal data that the controller sells to or shares with third parties, if any,
- the categories of third parties, if any, with whom the controller sells or shares personal data,
- the controller's contact information, including an active email address or other online mechanism that the consumer may use to contact the controller,
- a description of the controller's retention policies for personal data, and
- the date the privacy notice was last updated.

If a controller sells personal data to third parties, processes personal data for targeted advertising, or engages in certain profiling activities, the controller must disclose the processing in the privacy notice and provide access to a clear and conspicuous method (outside the privacy notice) for a consumer to their opt-out rights. This method may

include, but is not limited to, 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 web page where the consumer can make the opt-out request.

The privacy notice must be made available to the public in each language in which the controller provides a product or service that is subject to the privacy notice or carries out activities related to the product or service. The controller must provide the privacy notice in a manner that is reasonably accessible to and usable by individuals with disabilities, although the MCDPA does not mandate compliance with any particular accessibility standard, such as WCAG. The MCDPA also sets forth a framework for how, and under what circumstances, changes to the privacy policy must be conveyed to a consumer.

A controller is not required to provide a separate Minnesota-specific privacy notice or section of a privacy notice if the controller's general privacy notice contains all the information required by this section.

A controller that does not operate a website shall make the privacy notice conspicuously available to consumers through a medium regularly used by the controller to interact with consumers, including, but not limited to, mail.

Recordkeeping and Internal Policies

Pursuant to the MCDPA, a "controller must document and maintain a description of the policies and procedures the controller has adopted to comply" with the law, which must include, where applicable, a description of the controller's data privacy policies and procedures designed to:

- reflect the requirements of the MCDPA in the design of the controller's systems,
- identify and provide personal data to a consumer as required by this chapter,
- establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data, including the maintenance of an inventory of the data that must be managed to exercise the responsibilities under this item,
- limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data are processed,
- prevent the retention of personal data that is no longer relevant and reasonably necessary in relation to the purposes for which the data were collected and processed, and
- identify and remediate legal noncompliance.

This documentation must also identify the name and contact information of its chief privacy officer or other senior privacy officials within the company. Accordingly, although not explicit, the law seems to imply that organizations need to appoint a chief privacy officer or formally delegate authority to oversee privacy-related compliance matters to a senior official.

Information Security and Data Protection Assessments

The MCDPA requires a controller to "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data, including the maintenance of an inventory of the data that must be managed to exercise these responsibilities." These practices must be "appropriate to the volume and nature of the personal data at issue." Further, a controller and processor must "establish a clear allocation of the responsibilities between" them to implement appropriate technical and organizational measures. In addition, a controller may not retain personal data that is no longer relevant and reasonably necessary.

Pursuant to the MCDPA, a controller must conduct and document a data privacy and protection assessment for each of the following processing activities involving personal data:

- the processing of personal data for purposes of targeted advertising,
- the sale of personal data,
- the processing of sensitive data,
- any processing activities involving personal data that present a heightened risk of harm to consumers, and
- the processing of personal data for purposes of profiling, where the profiling presents a reasonably

> foreseeable risk of (i) unfair or deceptive treatment of, or disparate impact on, consumers, (ii) financial, physical, or reputational injury to consumers, (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person, or (iv) other substantial injury to consumers.

A data privacy and protection assessment must consider the type of personal data to be processed, including if sensitive data is involved. It "must identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the potential risks."

Data privacy and protection assessments or risk assessments conducted by a controller for compliance with other laws or regulations may qualify under this section if the assessments have a similar scope and effect, and a single assessment may address multiple sets of comparable processing operations that include similar activities.

Importantly, the MCDPA sets forth a framework for how controllers must disclose these assessments to the regulatory authorities.

Processor Obligations and Data Processing Agreements

The MCDPA places affirmative obligations on processors, including "adhering to the instructions of the controller" and "assisting the controller to meet" its legal obligations. Specifically, a processor must assist a controller by (i) responding to data subject requests, (ii) securing personal data and reporting data breaches, and (iii) undertaking data privacy and protection assessments.

The law requires controllers and processors to execute agreements (often called "data processing agreements") that set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. In addition, pursuant to the terms of these contracts, a processor (i) must ensure the confidentiality of its personnel, (ii) can only engage a subcontractor after coordination with the controller provided the subcontractor also agrees to data processing terms and conditions, (iii) has to agree to certain audits, compliance, and inspection provisions, and (iv) must delete or return the controller's personal data upon completion of the processing.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Thora Knight, Ph.D.
212.908.3971
Thora.Knight@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)