Featured Professionals

Sten-Erik Hoidal, CIPP

Related Services

Data Protection &
Cybersecurity

Technology & Data

Comprehensive Consumer Privacy Legislation Introduced in Minnesota

Legal Update
02.24.2021

On February 22, 2021, Representative Steve Elkins introduced a major new privacy bill (HF 1492) in the Minnesota House of Representatives containing significant privacy obligations for businesses to which it applies. Titled the Minnesota Consumer Data Privacy Act (MCDPA), the bill borrows from the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), and is specifically modeled after the Washington Privacy Act that is currently being considered by the Washington legislature. The full text of the MCDPA is available here, and the key provisions are summarized below. Look for future updates from Fredrikson & Byron as the MCDPA makes its way through the Minnesota Legislature.

Scope

The MCDPA provides new rights to "consumers," defined as Minnesota residents "acting only in an individual or household context" (and, presumably, not in their capacity as an employee). The MCDPA imposes corresponding obligations on entities that conduct business in Minnesota, or produce products or services targeted to residents of Minnesota, and that satisfy one or more of the following thresholds:

1. During a calendar year, control or process personal data of 100,000 consumers or more; or

2. Derive over 25 percent of gross revenue from the sale of personal data and process or control personal data of 25,000 consumers or more.

Note that definition of "sale" is not limited to the exchange of personal data for monetary consideration, but includes an exchange for "any other valuable consideration."

Certain types of businesses and data are exempt under the MCDPA. For example, it does not apply to governmental entities, federally recognized Indian tribes, or personal data that is regulated under HIPAA, Gramm-Leach-Bliley, the Fair Credit Reporting Act, or the Family Educations Rights and Privacy Act. Unlike the CCPA, however, the MCDPA does not include an exemption for nonprofit entities (though, as discussed below, they would have a substantially longer time to come into compliance).

Controllers and Processors' Obligations

Obligations under the MCDPA are imposed on "controllers" and "processors"—concepts borrowed from the GDPR. A "controller" is the "natural or legal person that, alone or jointly with others, determines the purposes and means of processing personal data." A processor, in turn, is the "natural or legal person who processes personal data on behalf of a controller." Determining whether an entity is controller or processor under the MCDPA is "a fact-based determination that depends upon the context in which personal data are to be processed."

The MCDPA requires the activities of a processor to be governed by a contract with the controller. The contract should identify, among other things, the instructions to which the processor is bound, including "the nature and purpose of the processing, the type of personal data subject to the processing, the duration of the processing, and the obligations and rights of both parties."

A processor is responsible for assisting a controller in meeting its obligations under the MCDPA and must ensure that each person processing personal data is bound by a duty of confidentiality. The processor can only engage a subcontractor if certain requirements are met and it provides the controller with an opportunity to object to the subcontractor. Further, the processor must allow for and contribute to reasonable inspections by the controller or the controller's auditor.

In addition to operationalizing the consumer rights discussed below, a controller must provide a privacy notice that identifies the following:

1. the categories of personal data it processes;
2. the purposes of which those categories are processed;
3. how and where consumers may exercise their rights under the MCDPA and appeal the controller's action;
4. the categories of personal data shared with third parties; and
5. the categories of third parties with whom the controller shares personal data.

In addition, the MCDPA contains certain restrictions on a controller's collection of personal data, including that it be "limited to what is reasonably necessary in relation to the purposes for which such data are processed, as disclosed to the consumer." A controller is also required to implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data.

Consumer Rights and Appeal Process

Similar to the GDPR and CCPA, the MCDPA grants consumers five rights relating to their personal data:

1. **Access**. The right to confirm whether a controller is processing data about the consumer and access the data being processed.
2. **Correction**. The right to correct inaccurate personal data.
3. **Deletion**. The right to delete personal data about the consumer.
4. **Portability**. The right to obtain copies of personal data about the consumer in a portable, usable and transferrable format.
5. **Opt out**. The right to opt out of processing of personal data for the purposes of targeted advertising, the sale of personal data and certain types of profiling.

A consumer may exercise these rights at any time by submitting a request to a controller and identifying the rights the consumer wishes to exercise. A controller has 15 days to process opt out requests and 45 days to process all other requests. In certain circumstances, the 45-day response period may be extended by an additional 45 days.

A controller must also establish a process allowing consumers to appeal the controller's denial of, or refusal to act on, a request to exercise rights. If a consumer submits an appeal, the controller must respond within 30 days of receipt explaining the reasons supporting any action taken on the appeal. This period can be extended for an additional 60 days where necessary. In responding to an appeal, the controller must also inform the consumer how to file a complaint with the Minnesota Attorney General.

Prohibition on Discrimination

The MCDPA contains two non-discrimination provisions applicable to controllers. First, a controller is prohibited from processing personal data based on certain actual or perceived characteristics (e.g., race, color, ethnicity, religion, gender, etc.) in a manner that would unlawfully discriminate against consumers with respect to the provision of housing, employment, credit, education or public accommodations.

Second, a controller is prohibited from discriminating against a consumer for exercising any rights available under the MCDPA. Specifically, a controller cannot refuse to provide, charge different prices or rates, or provide different quality goods or services because a consumer exercised rights under the Act. This prohibition does not apply to certain bona fide loyalty and rewards programs.

Data Protection Assessments

Similar to GDPR, the MCDPA requires controllers to conduct "data protection assessments" for certain processing activities, including processing personal data in connection with targeted advertising, personal data sales, processing sensitive data, profiling that could be deceptive or injurious to consumers, or that otherwise presents a heightened risk of harm to consumers.

Fredrikson

The purpose of the data protection assessment is to analyze and compare the benefits that the controller, consumer or other stakeholders (including the public) may receive from the proposed processing against the potential risks the processing presents to the rights of the consumer. The controller must document and should retain its data protection assessments. The controller must make a data protection assessment available to the Minnesota Attorney General upon request, if relevant to an investigation.

Enforcement

The Minnesota Attorney General is responsible for enforcement of the MCDPA. As currently written, it does not include a private right of action. Prior to bringing an enforcement action, the Attorney General must provide the controller or processor with a warning letter identifying the specific provisions of the MCDPA that it alleges have been violated. The controller or processor will then have 30 days to cure those deficiencies before the Attorney General commences enforcement. Violations of the MCDPA are subject to injunctive relief and civil penalties up to $7,500 per violation.

Effective Date

The MCDPA has a proposed effective date of July 31, 2022. Nonprofits organized under Minnesota law, air carriers and postsecondary educational institutions would not be required to comply until July 31, 2026.