Bill Summary

H.F. 2309

Second engrossment

Subject	Minnesota Consumer Data Privacy Act
Authors	Elkins and others
Analyst	Nathan Hopkins
Date	March 7, 2024

Overview

This bill regulates businesses' use of personal data on individuals. It also gives Minnesotans various rights regarding their personal data.

The European Union adopted its comprehensive data privacy law, the General Data Protection Regulation (GDPR), in 2016. The United States, however, still lacks a national comprehensive data privacy law. This has prompted various states to develop their own. In 2018, California passed its California Consumer Privacy Act (CCPA), which was expanded in 2020 by the California Privacy Rights Act (CPRA). The CCPA and CPRA were inspired by the GDPR and have become the foundational comprehensive data privacy laws in the United States. Since then, 11 other states have passed their own data privacy laws generally modeled after CCPA/CPRA. If passed, this bill would create such a privacy law for Minnesota.

Summary

Section	Description
1	**Attorney general data coded elsewhere.** Creates a cross-reference in the Minnesota Government Data Practices Act regarding the classification of "data privacy and protection assessments" that may be maintained by the Minnesota attorney general under section 9 of the bill. That section classifies these assessments as nonpublic data.
2	**Citation.** Codifies a new chapter of statute, chapter 3250, that may be referred to as the "Minnesota Consumer Data Privacy Act."
3	**Definitions.** Defines key terms for the act, the following of which may be especially noteworthy. ▪ "Personal data" means information that can be linked to a particular natural person. In addition, "sensitive personal" data is a defined term

Section	Description

including certain forms of personal data in which individuals may have a heightened privacy interest.

- "Processing" means any action performed on personal data: its collection, storage, disclosure, analysis, etc.
- "Profiling" means automated processing of a person's data—through the application of algorithms or artificial intelligence, for example—to predict, evaluate, or analyze the person.
- A "controller" is an entity that determines how personal data is processed, while a "processor" is an entity that processes personal data on behalf of a controller.
- A "consumer" means a natural person residing in Minnesota. It does not include a natural person acting in a commercial or employment context.
- "Sale" means exchange of personal data for money or other consideration. Certain kinds of disclosures of personal data are exempted from the definition of sale.

4 **Scope; exclusions.**

Subd. 1. Scope. Specifies what kind of legal entities are subject to the act. Includes entities that conduct business in Minnesota or offer products/services to Minnesota residents. Sets a threshold based upon an entity's level of involvement with the personal data of consumers (i.e. Minnesota residents).

Subd. 2. Exclusions. Excludes certain types of entities and data from the act. Government entities and Indian Tribes are excluded. Also, in general, processing of personal data that is already subject to heightened privacy regulation at the federal level (e.g. health data, certain financial data, etc.) is excluded.

5 **Responsibility according to role.**

Places certain obligations on controllers and processors, regarding their relationship to each other and regarding individuals whose personal data is being processed. This includes implementing data security measures and ensuring compliance with the act. How to determine whether a person is a controller or a processor with respect to certain data is addressed in paragraph (g).

6 **Consumer personal data rights.**

Subd. 1. Consumer rights provided. Gives consumers six rights regarding their personal data:

1) a right to know and access personal data processed by a controller;
2) a right to correct inaccurate personal data;
3) a right to delete personal data;
4) a right to obtain a copy of the consumer's personal data;

Section	Description

5) a right to opt out of:
    i) the processing of personal data for purposes of targeted advertising;
    ii) the sale of personal data; or
    iii) profiling that has certain significant consequences; and
6) a right to review, understand, question, and correct how personal data has been profiled.

Subd. 2. Exercising consumer rights. Allows the consumer to exercise rights provided under subdivision 1 by sending a request to controller.

Subd. 3. Universal opt-out mechanisms. Requires controllers to honor consumer requests sent via an external "universal" platform, technology, or mechanism.

Subd. 4. Controller response to consumer requests. Requires controllers to provide a reliable, accessible way for consumers to exercise their rights under subdivision 1. Sets a 45-day time limit for complying with a request to exercise consumer rights. Allows controllers to deny fraudulent requests and charge fees before responding to certain unfounded or excessive requests.

Subd. 5. Appeal process required. Requires a controller to establish an internal appeal process if a consumer's request to exercise a right is denied. Sets a 45-to-105-day time limit for appeals. If a consumer appeal is denied, the controller must provide information on how to file a complaint with the Minnesota attorney general.

7 **Processing deidentified or pseudonymous data.**

"Deidentified data" and "pseudonymous data" are defined terms in the act. This section essentially allows a controller to create and utilize deidentified or pseudonymous data derived from personal data, and limits consumer's ability to exercise rights over such truly deidentified or pseudonymous data.

8 **Responsibilities of controllers.**

Subd. 1. Transparency obligations. Requires a controller to provide consumers with a privacy notice explaining: what personal data are processed, sold, shared, or profiled by the controller; how long personal data is retained by the controller; and the consumer's rights over their personal data. Sets other requirements for the privacy notice.

Subd. 2. Use of data. Limits a controller's ability to collect and use personal data. Requires appropriate data security practices. Prohibits the processing of sensitive data (a defined term) without consumer consent, which may be revoked. For

Section	Description
	children between 13 and 16, prohibits targeted advertising and prohibits the sale of personal data without consent. **Subd. 3. Nondiscrimination.** Prohibits controllers from processing of personal data based on certain protected classifications (race, gender, etc.) in a way that discriminates against consumers of that class in certain significant areas (housing, employment, public accommodation, etc.). Prohibits controllers from discriminating against consumers for exercising their rights under this act. Limits the sale of personal data as part of a controller's loyalty, rewards, and benefits program. **Subd. 4. Waiver of rights unenforceable.** Prohibits contracts that seek to have consumers waive their rights under the act.
9	**Requirements for a small business.** Prohibits a small business from selling a consumer's "sensitive data," a defined term under the act, without the consumer's permission. Penalties and enforcement provisions of the act generally apply to a small business that violates this section. Small businesses are exempt from the act generally under section 4, subdivision 2, but this section applies specifically to them.
10	**Data privacy and protection assessments.** Requires controllers to create "data privacy and protection assessments" to describe policies and procedures that show compliance with the act. Sets requirements for the assessment. Allows the attorney general to request copies of the assessments that relate to ongoing investigations.
11	**Limitations and applicability.** Limits the application of the act to avoid conflict with certain other laws or interference with certain appropriate business practices.
12	**Attorney general enforcement.** Allows the attorney general to bring a civil lawsuit under its existing authority against a controller or processor that violates the act. Provides civil penalties of up to $7,500 for each violation. Requires the attorney general to issue a warning letter and provide an opportunity to cure the violation before bringing the civil lawsuit.
13	**Preemption of local law; severability.** Supersedes and preempts any local laws regarding the processing of personal data by controllers and processors. If a portion of the act is found invalid by the courts, allows the remainder of the act to stay in force.

Section	Description
14	**Effective date.** Provides an effective date of July 31, 2025. Nonprofit corporations and postsecondary institutions are not required to comply until July 31, 2029.