February 25, 2026

RE: (As-Introduced Version) HF 2700 - Minnesota Consumer Data Privacy Act modified to make consumer health data a form of sensitive data, and additional protections added for sensitive data

Rep. Elkins, Chair Koegel, Chair O'Driscoll, and Members of the House Commerce Committee:

On behalf of retailers across the state, we appreciate the opportunity to provide feedback on HF 2700. We share the goal of protecting consumer data and recognize the importance of strong, clear privacy standards. Minnesota has taken thoughtful steps in this space, and we value the collaborative approach that led to the current framework. We understand an amendment is being drafted, so please note these comments are drafted to the introduced version of the bill.

We appreciate the attempt to align Minnesota's law with updates from Washington and Connecticut into a single privacy framework. Adopting Connecticut's protections for health data will be much clearer, as those provisions were drafted to operate within a comprehensive privacy framework similar to Minnesota's. By contrast, Washington's My Health My Data approach was developed outside of a broader framework, and incorporating it here appears to create misalignment. As a result, the bill introduces overbroad definitions and highly prescriptive authorization requirements that extend beyond identifiable health information. We suggest any updates should be more directly tied back to Minnesota's existing statutory definitions and structure, following the Connecticut language that adds on to an existing privacy law, to avoid duplication and unintended scope expansion.

As such, HF 2700 significantly expands the scope of the Minnesota Consumer Data Privacy Act in ways that extend well beyond traditional consumer data protections and into routine retail operations. We are concerned that several provisions, particularly those related to "sensitive data" and "health data," create unintended consequences for retailers and the customers they serve.

1. Expansion of “Health Data” and “Sensitive Data” (Section 325M.11)

HF 2700 substantially broadens the definition of “health data” and incorporates it into “sensitive data.” The definition includes not only medical information, but also inferred or derived data and consumer interactions such as the purchase of medications, browsing for health-related products, or location data that could suggest a healthcare visit.

For retailers, this creates significant ambiguity and risk. Everyday transactions—such as purchasing over-the-counter medication, vitamins, or personal care products—could be classified as sensitive data processing. In addition, modern retail analytics tools that infer consumer preferences may unintentionally fall within this definition. This expansion risks sweeping in standard retail activity that consumers would not reasonably consider “health data.”

2. Layered and Prescriptive Consent Requirements (Section 325M.16, subdivision 2)

The bill establishes multiple, distinct consent requirements for processing, sharing, and selling sensitive data, including a requirement that consent be separate and specific for each use.

While transparency is important, these layered requirements introduce significant operational complexity. Retailers would need to redesign customer interfaces, loyalty programs, and marketing systems to accommodate multiple consent flows. This could lead to consumer confusion, consent fatigue, and reduced participation in programs that provide value to customers.

We are particularly concerned that standard retail practices—such as personalized offers or communications based on purchase history—could be subject to heightened consent requirements if any data element is interpreted as “sensitive.”

3. Restrictions on the Sale of Sensitive Data (Section 325M.175)

HF 2700 creates a highly prescriptive authorization framework for the sale of sensitive data, requiring a standalone written authorization with detailed disclosures, named third parties, and a one-year expiration.

While we understand the intent, this approach is operationally impractical and does not align with how data flows in modern retail ecosystems. It also creates uncertainty around what constitutes a “sale” versus routine data sharing with service providers, advertising

partners, or analytics vendors. Without clearer boundaries, retailers face increased legal risk even when engaging in standard business practices.

4. Geofencing Restrictions (Section 325M.178)

The prohibition on geofencing around healthcare locations raises concerns due to its breadth and ambiguity. Retailers and their marketing partners may not always have visibility into how location-based advertising tools operate, particularly when managed by third-party platforms.

Without clear definitions and guardrails, retailers could face liability for activities outside of their direct control. We encourage clarification to ensure that compliant businesses are not unintentionally exposed to enforcement risk.

5. Expanded Applicability to Businesses of All Sizes (Section 325M.175, subdivision 1)

The bill applies sensitive data requirements broadly, regardless of whether a business meets the existing thresholds in current law. This effectively brings small and mid-sized retailers into scope if they handle any data that could be interpreted as sensitive.

This expansion significantly increases the compliance burden across the retail sector, particularly for businesses that do not have dedicated legal or privacy teams.

6. Data Minimization, Inventory, and Retention Requirements (Section 325M.16)

The bill reinforces requirements to limit data collection, maintain inventories, and delete data when no longer necessary. While these are important principles, implementation will require substantial operational changes, particularly for retailers managing complex customer data systems across multiple platforms.

7. Mandatory Data Privacy and Protection Assessments (Section 325M.18)

The requirement to conduct and document assessments for targeted advertising, profiling, and sensitive data processing introduces a significant compliance obligation. These assessments may be subject to review by the Attorney General, further increasing the need for legal and technical resources.

8. Enforcement Changes (Section 325M.20)

The expiration of the 30-day cure period after January 31, 2026 increases enforcement risk. Given the complexity and ambiguity introduced by this bill, retailers may face penalties for unintentional violations without an opportunity to correct issues.

Minnesota Retailers supports strong, workable consumer data protections. However, HF 2700, as drafted, extends beyond its intended scope and risks capturing routine retail activity in a way that creates confusion, compliance challenges, and potential disruption to customer experiences.

We would welcome the opportunity to work with Rep. Elkins and the committee to:

- Clarify the definition of “health data” to better align with consumer expectations
- Ensure that consent requirements are workable and do not create unnecessary friction
- Provide clearer distinctions between “sale” and standard business data sharing
- Refine geofencing provisions to avoid unintended liability
- Align applicability thresholds to avoid disproportionate impacts on smaller retailers

Thank you for your consideration and for your continued work on consumer data privacy. We look forward to being a constructive partner in refining this legislation.

Sincerely,

Bruce Nustad
president
bruce@mnretaill.org