MINNESOTA DATA FAIRNESS ACT (DFA)

Prepared By M.D.T

An act relating to consumer data governance; proposing coding for new law in Minnesota Statutes, chapter 13; establishing the Minnesota Data Fairness Act; regulating data monetization; requiring transparency, accountability, and fair participation to reduce systemic uncertainty and restore legitimate public trust.

Purpose: Establish enforceable digital rights and predictable rules for personal data collection, use, profiling, automated decision systems, and data monetization, while protecting Minnesotans from coercive consent, unfair exclusion, and discriminatory outcomes.

Implementation: This act provides clear compliance duties, transparent oversight, and meaningful remedies designed to reduce systemic uncertainty and volatility by restoring legitimate trust in data-driven systems.

Section 1. [13.901] SHORT TITLE.
Subdivision 1.
This act may be cited as the Minnesota Data Fairness Act.

Sec. 2. [13.902] PURPOSE AND LEGISLATIVE FINDINGS.
Subdivision 1. Purpose.
The purpose of this act is to:
(1) establish a Digital Bill of Rights for Minnesota residents;
(2) regulate the collection, processing, transfer, and monetization of personal data in a transparent and predictable manner;
(3) protect individuals against harmful profiling and opaque automated decision systems affecting access to opportunity; and
(4) ensure individuals may participate fairly in economic value created from the use of their personal data.

Subd. 2. Legislative findings.
(1) personal data has measurable economic value and is routinely monetized without meaningful transparency or voluntary consent;
(2) existing state and federal laws do not provide a comprehensive framework for data monetization and algorithmic accountability;
(3) unchecked data practices can create systemic risk, including discriminatory profiling, unfair pricing, and exclusion from housing, credit, employment, health care, and other essential services;
(4) Minnesotans have a right to digital self-determination, including control over how their data is collected, used, and monetized;
(5) public trust is a critical component of stable, effective governance in data-driven systems; and
(6) systems relying on opaque data practices, coerced consent, or unaccountable automation increase institutional risk, public resistance, and regulatory volatility, whereas systems grounded in transparency, fairness, and enforceable rights reduce uncertainty at its source by fostering trust,

voluntary cooperation, and long-term stability.

Subd. 3. Constitutional findings.
(1) concentrated power, whether exercised by public or private actors, threatens liberty and requires structural limitations and enforceable rights;
(2) separation of powers and due process protections were designed to prevent consolidation of decision-making and economic control;
(3) large-scale data collection, profiling, and automated decision systems, when deployed without clear limits or accountability, may materially affect constitutional interests including due process and equal protection;
(4) consent obtained through necessity, dependency, or lack of reasonable alternatives may not constitute meaningful consent; and
(5) this act operates as a rights-protective, risk-reduction framework consistent with constitutional limits and does not restrict lawful speech, innovation, or commerce.

Sec. 3. [13.903] DEFINITIONS.
Subdivision 1. Scope.
For purposes of sections 13.901 to 13.916, the terms defined in this section have the meanings given.
Subd. 2. Personal data.
“Personal data” means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable individual.
Subd. 3. Sensitive data.
(1) health or medical information;
(2) biometric identifiers;
(3) precise geolocation information;
(4) financial account numbers and access credentials;
(5) government-issued identifiers;
(6) personal data of a known minor; or
(7) information revealing protected characteristics under state or federal law.
Subd. 4. Data monetization.
“Data monetization” means any sale, license, lease, transfer for consideration, sharing for targeted revenue, or other revenue-generating use of personal data, whether direct or indirect.
Subd. 5. Data broker.
“Data broker” means a person or entity whose primary business purpose is collecting, aggregating, selling, licensing, or otherwise monetizing personal data not collected directly from the individual.
Subd. 6. Profiling.
“Profiling” means automated processing of personal data to evaluate, analyze, or predict aspects concerning an individual’s economic situation, health, interests, behavior, preferences, reliability, location, or access to opportunities.
Subd. 7. Automated decision system.
“Automated decision system” means a computational process, including a system derived from machine learning or statistical modeling, that makes, recommends, or materially assists a decision that produces

legal or similarly significant effects for an individual.

Subd. 8. Controller; processor.

“Controller” means a person or entity that determines the purposes and means of processing personal data.

“Processor” means a person or entity that processes personal data on behalf of a controller.

Subd. 9. Consent.

“Consent” means a freely given, specific, informed, and unambiguous indication of an individual’s wishes by which the individual, by a clear affirmative act, signifies agreement to the processing or monetization of personal data for a defined purpose, sufficient to support legitimate reliance by both the individual and the controller.

Subd. 10. Essential goods and services.

“Essential goods and services” includes housing, employment, education, health care, insurance, financial services, utilities, telecommunications, and other services where denial or degradation materially affects basic living conditions.

Sec. 4. [13.904] INDIVIDUAL DIGITAL RIGHTS.

Subdivision 1. Rights guaranteed.

(1) right to confirm whether a controller processes personal data concerning the individual;

(2) right to access personal data and a meaningful explanation of its categories, sources, purposes, and recipients;

(3) right to correct inaccurate personal data;

(4) right to delete personal data, subject to lawful retention requirements;

(5) right to data portability, including a copy in a readily usable format;

(6) right to revoke consent at any time without penalty or retaliation;

(7) right to opt in to data monetization and to withdraw that opt-in; and

(8) right to meaningful human review of an adverse decision produced by an automated decision system.

Subd. 2. Methods for exercising rights.

A controller must provide clear, accessible, and free methods for an individual to exercise rights under this act, including at minimum a secure online request mechanism and an alternative method reasonably accessible to individuals with disabilities.

Subd. 3. Response timelines.

A controller must respond to an authenticated request within 45 days, with a one-time extension of 45 additional days when reasonably necessary, provided the controller informs the individual of the extension and the reason for it.

Subd. 4. Appeals.

If a controller denies a request, the controller must provide a written explanation and a method to appeal the decision. A controller must decide an appeal within 45 days.

Sec. 5. [13.905] LIMITATIONS ON DATA COLLECTION AND USE.

Subdivision 1. Data minimization.

A controller shall collect and process personal data only to the extent that the data is reasonably necessary and proportionate to accomplish a disclosed purpose.

Subd. 2. Purpose limitation.
A controller shall not process personal data for a purpose materially different from the disclosed purpose without obtaining renewed consent.
Subd. 3. Retention limits.
A controller shall not retain personal data longer than reasonably necessary for the disclosed purpose, unless retention is required by law.
Subd. 4. Prohibition of dark patterns.
A controller shall not obtain consent through dark patterns, deception, coercion, or unreasonable conditions that materially impair voluntary choice. Consent obtained through such means is invalid.
Subd. 5. Sensitive data and minors.
Processing of sensitive data requires affirmative express consent. A controller shall provide heightened protections for data concerning minors, including limits on profiling and monetization.

Sec. 6. [13.906] DATA MONETIZATION AND FAIR PARTICIPATION.
Subdivision 1. Opt-in required for monetization.
A controller shall not monetize personal data unless the individual has provided opt-in consent specific to monetization.
Subd. 2. Monetization disclosures.
A controller engaging in data monetization shall disclose:
(1) categories of personal data to be monetized;
(2) purposes of monetization;
(3) categories of third parties receiving monetized data;
(4) the duration of monetization authorization; and
(5) the method by which the individual may revoke monetization consent.
Subd. 3. Fair participation mechanisms.
Where a controller derives material economic value from monetized personal data, the controller shall provide a fair participation mechanism. A fair participation mechanism may include monetary compensation, service credits, reduced pricing, dividends, or other measurable benefits.
Subd. 4. Recordkeeping.
A controller engaging in data monetization must maintain records sufficient to demonstrate compliance, including consent records, disclosures, and categories of third-party recipients, for at least five years.

Sec. 7. [13.907] PROFILING AND AUTOMATED DECISION ACCOUNTABILITY.
Subdivision 1. Notice.
A controller shall provide clear notice when profiling or an automated decision system is used to make or materially assist a decision producing legal or similarly significant effects.
Subd. 2. Explanation.
Upon request, a controller shall provide a meaningful explanation of the principal factors, data categories, and logic used by the automated decision system, to the extent such disclosure does not require revealing trade secrets, provided the explanation must be sufficient to allow the individual to understand the basis of the decision and to meaningfully contest it.
Subd. 3. Human review and appeal.
An individual has the right to obtain human review of an adverse decision and to present additional

information. The controller must designate a qualified reviewer with authority to override or modify the automated output.

Subd. 4. Nondiscrimination.

A controller shall not process personal data in a manner that results in unlawful discrimination or that circumvents civil rights protections.

Subd. 5. Risk assessments.

A controller that uses profiling or automated decision systems for high-impact decisions shall conduct and document periodic risk assessments, including evaluation of bias, accuracy, security, and potential harm, and implement mitigation measures.

Sec. 8. [13.908] DATA BROKER REGISTRATION AND DISCLOSURE.

Subdivision 1. Registration required.

A data broker conducting business in Minnesota or collecting personal data of Minnesota residents shall register annually with the commissioner of commerce.

Subd. 2. Registration contents.

Registration must include:

(1) legal name and any trade names;

(2) primary business address and contact information;

(3) categories of personal data collected and sold;

(4) categories of purchasers or recipients; and

(5) a method for individuals to submit access, deletion, and opt-out requests.

Subd. 3. Public registry.

The commissioner shall maintain a public, searchable registry of registered data brokers.

Sec. 9. [13.909] SECURITY AND BREACH NOTIFICATION.

Subdivision 1. Safeguards.

A controller and processor shall implement reasonable administrative, technical, and physical safeguards appropriate to the volume and sensitivity of the data, including access controls, encryption where appropriate, and secure disposal.

Subd. 2. Breach notification.

In the event of a security breach involving personal data, a controller shall notify affected individuals and the attorney general without unreasonable delay and, where feasible, within 72 hours after discovery, consistent with applicable state law.

Subd. 3. Content of notice.

Notice must include the categories of data involved, the approximate date range of the breach if known, the steps taken to mitigate harm, and steps an individual can take to protect against identity theft or other misuse.

Sec. 10. [13.910] ENFORCEMENT.

Subdivision 1. Attorney general authority.

The attorney general may investigate violations of sections 13.901 to 13.916 and may bring an action to obtain injunctive relief, restitution, civil penalties, and other relief authorized by law.

Subd. 2. Civil penalties.

A court may impose civil penalties for violations, taking into account the nature and number of violations, the size and resources of the violator, the degree of culpability, and the extent of harm.

Subd. 3. Cure period.

For non-willful violations, the attorney general may provide a reasonable opportunity to cure before seeking civil penalties, except where cure is not feasible or where the violation involves sensitive data, minors, or repeated misconduct.

Sec. 11. [13.911] PRIVATE RIGHT OF ACTION.

Subdivision 1. Civil action.

An individual harmed by a violation of sections 13.901 to 13.916 may bring a civil action in a court of competent jurisdiction.

Subd. 2. Remedies.

Available remedies include actual damages, injunctive relief, declaratory relief, and reasonable attorney fees and costs.

Subd. 3. Nonwaiver.

A purported waiver of rights under this act is void as against public policy.

Sec. 12. [13.912] DATA IMPACT ASSESSMENTS.

Subdivision 1. Required assessments.

A controller engaged in high-risk processing, including profiling or automated decision systems affecting essential goods and services, shall conduct an annual data impact assessment.

Subd. 2. Minimum contents.

A data impact assessment must include:

(1) description of processing activities and purposes;

(2) categories of personal data used;

(3) necessity and proportionality analysis;

(4) risk analysis for privacy, security, discrimination, and exclusion; and

(5) mitigation measures and monitoring plan.

Subd. 3. Availability to regulator.

A controller shall provide an assessment to the commissioner or attorney general upon request.

Sec. 13. [13.913] NON-RETALIATION.

Subdivision 1. Prohibited retaliation.

A controller shall not retaliate against an individual for exercising rights under this act, including by denying goods or services, charging different prices, providing a different level or quality of goods or services, or imposing unreasonable burdens to exercise rights.

Subd. 2. Permissible differences.

A controller may offer a voluntary loyalty or benefits program only if its terms are disclosed and the program is not used to coerce consent for monetization or to penalize the exercise of rights.

Sec. 14. [13.914] TRANSPARENCY IN ALGORITHMIC SYSTEMS.

Subdivision 1. Plain-language disclosures.

A controller that deploys automated decision systems for high-impact decisions shall provide plain-language disclosures describing the system’s purpose, the categories of data used, and the general

types of outcomes the system influences.

Subd. 2. Meaningful appeal.

A controller shall provide a meaningful appeal process, including human review, for individuals subject to adverse decisions.

Sec. 15. [13.915] RULEMAKING AUTHORITY.

Subdivision 1. Authority.

The commissioner of commerce may adopt rules necessary to implement sections 13.901 to 13.916, including rules establishing forms, disclosures, and procedures consistent with this act.

Subd. 2. Coordination.

The commissioner may coordinate with the attorney general and other relevant agencies to ensure consistent enforcement guidance.

Sec. 16. [13.916] EFFECTIVE DATE.

Subdivision 1. Effective date.

Sections 13.901 to 13.916 are effective January 1, 2026.

Subd. 2. Applicability.

This act applies to personal data collected, processed, or monetized on or after the effective date.