DATA DISTRIBUTION FAIRNESS ACT (DDFA)

Official Legislative Draft

Prepared by M.D.T

DATA DISTRIBUTION FAIRNESS ACT (DDFA)
A bill for an act relating to consumer data privacy; proposing coding for new law in Minnesota Statutes, chapter 13; establishing the Data Distribution Fairness Act; regulating data monetization; requiring transparency, accountability, and fair economic participation.

Section 1. [13.901] SHORT TITLE.

This act may be cited as the “Data Distribution Fairness Act.”

Sec. 2. [13.902] PURPOSE AND LEGISLATIVE FINDINGS.

Subdivision 1. Purpose.
The purpose of this act is to:

Establish a Digital Bill of Rights for Minnesota residents;

Regulate the monetization, transfer, and reuse of personal data;

Protect individuals against harmful profiling and opaque automated decision systems; and

Ensure that individuals may participate fairly in the economic value created from the use of their personal data.

Subd. 2. Legislative findings.
The legislature finds that:

Personal data collected from Minnesotans has measurable economic value and is routinely monetized without meaningful transparency, consent, or compensation.

Existing state and federal laws do not provide a comprehensive framework for data governance, data monetization, and algorithmic accountability.

The unchecked use of personal data can enable discriminatory profiling, unfair pricing, and exclusion from housing, credit, employment, health care, and other essential services.

Minnesotans have a right to digital self-determination, including control over how their data is collected, used, and monetized, and a right to participate in the economic value their data generates.

Clear rules, enforceable rights, and meaningful remedies are necessary to restore public trust in digital systems and prevent exploitation in the data economy.

Sec. 3. [13.903] DEFINITIONS.

For purposes of sections 13.901 to 13.916, the following terms have the meanings given:

“Personal data” means any information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, to an identified or identifiable individual, including derived, inferred, or behavioral data.

“Sensitive data” includes, but is not limited to, data relating to an individual’s health

status, genetic or biometric identifiers, precise geolocation, racial or ethnic origin, religious affiliation, sexual orientation, union membership, immigration status, minors, and financial identity.

“Data broker” means any business or entity, other than an entity that collects data solely from its direct customers for internal operations, whose primary business model involves collecting, aggregating, licensing, selling, or otherwise distributing personal data it did not collect directly from the individual.

“Profiling” means any form of automated processing of personal data to evaluate, analyze, or predict aspects relating to an individual’s behavior, preferences, creditworthiness, work performance, economic situation, health, interests, reliability, or access to opportunities.

“Monetization” means any revenue-generating use of personal data, including sale, licensing, targeted advertising, data-sharing for consideration, or use of personal data as an input to products or services that generate revenue.

“Automated decision system” means a computational process, including one derived from machine learning, statistics, or artificial intelligence, that makes or materially assists in making decisions or recommendations that affect individuals’ rights, opportunities, or access to essential services.

“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.

Sec. 4. [13.904] INDIVIDUAL DIGITAL RIGHTS.

Subdivision 1. Rights established.
Minnesota residents have the following rights with respect to their personal data:

Right to transparency. To receive a clear and accessible explanation of what personal data is collected, from which sources, for what purposes, and with which categories of third parties it is shared or monetized.

Right of access. To obtain a copy of their personal data in a readily usable format.

Right to correction. To correct inaccurate, incomplete, or outdated personal data.

Right to deletion. To request deletion of personal data, subject to narrow, clearly defined exceptions such as legal obligations or security incident investigation.

Right to revocation of consent. To withdraw consent for processing or monetization at any time, without retaliation or degradation of core service.

Right to portability. To receive personal data in a portable, machine-readable format that enables transfer to another provider.

Right to fair compensation. To receive equitable economic participation when their personal data is monetized, consistent with section 13.906.

Right to algorithmic due process. To receive meaningful explanations and human review of significant automated decisions that affect housing, employment, credit, health, or access to essential services.

Subd. 2. Exercise of rights.
Controllers must provide at least one free, accessible mechanism—online and offline where feasible—for individuals to exercise these rights and must respond within 45 days, extendable once for an additional 45 days for complex requests with notice to the individual.

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

Data minimization. Controllers may collect and process only the personal data that is reasonably necessary and proportionate to the disclosed purpose.

Purpose limitation. Personal data collected for a specific purpose may not be used for incompatible secondary purposes, including monetization, without explicit opt-in consent from the individual.

Retention limits. Personal data must not be retained longer than necessary to fulfill the stated purpose, comply with law, or protect the security and integrity of systems.

Prohibition of dark patterns. Consent must be freely given, specific, informed, and unambiguous. Interfaces that use dark patterns or manipulative design to obtain consent are prohibited.

Children and sensitive data. Collection and use of children’s data and sensitive data require heightened safeguards and separate, explicit consent.

Sec. 6. [13.906] DATA MONETIZATION AND FAIR COMPENSATION.

Opt-in requirement. No controller or data broker may monetize an individual’s personal data without documented, opt-in consent that is separate from general terms of service.

Disclosure of monetization practices. Controllers must provide a clear, plain-language description of:

the types of monetization activities;

the categories of third parties receiving data; and

how individual compensation will be calculated.

Equitable compensation. Individuals whose data materially contributes to revenue-generating products or services are entitled to fair and proportional economic participation, which may include per-transaction payments, revenue-sharing pools, credits, or other transparent mechanisms.

Accounting and records. Controllers and data brokers must maintain records sufficient to demonstrate compliance with this section and provide such records to the Attorney General upon request.

Sec. 7. [13.907] PROFILING AND AUTOMATED DECISION ACCOUNTABILITY.

Explanation and notice. When an automated decision system is used in housing, employment, credit, health, insurance, education, or access to essential government or private services, the individual must receive a clear explanation of the role of the system and the key factors considered.

Human review. Individuals have the right to request timely human review of adverse decisions and to submit additional information relevant to the decision.

Prohibited profiling. Profiling that results in unlawful discrimination, disparate impact on protected classes, or unreasonable intrusion into personal autonomy is prohibited.

Risk assessment. Controllers that use automated decision systems with significant impact must conduct and regularly update documented risk assessments addressing bias, discrimination, privacy, and security.

Sec. 8. [13.908] DATA BROKER REGISTRATION.

Registration requirement. All data brokers operating in Minnesota must register annually with the Department of Commerce.

Disclosures. Registration must include:

categories and sources of personal data collected;

purposes of collection and monetization;

whether individuals may opt out or receive compensation; and

contact information for exercising rights.

Public registry. The department shall maintain a public, searchable registry of data brokers.

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

Security safeguards. Controllers and processors must implement reasonable administrative, technical, and physical safeguards appropriate to the sensitivity, volume, and risk associated with the personal data they hold.

Breach notification. In the event of a data breach involving personal data, affected individuals must be notified without unreasonable delay and, in any event, within 72 hours after confirmation of the breach, unless delayed by law enforcement necessity.

Liability for failure to safeguard. Failure to implement reasonable safeguards constitutes a violation of this act and may result in damages and civil penalties.

Sec. 10. [13.910] ENFORCEMENT.

Attorney General authority. The Attorney General may investigate violations of this act, issue civil investigative demands, compel production of documents and testimony, and bring civil actions to enforce compliance.

Civil penalties. Courts may impose civil penalties of:

up to $7,500 per violation involving personal data; and

up to $15,000 per violation involving minors' data or sensitive data.

Injunctive relief. Courts may issue temporary, preliminary, or permanent injunctions, including orders requiring deletion of unlawfully obtained data or suspension of data processing activities.

Cure period. For first-time, non-intentional violations, the Attorney General may allow a 30-day cure period after notice. The cure period does not apply to violations involving intentional misconduct, monetization of minors' data, or willful disregard of this act.

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

Civil remedy. A Minnesota resident whose rights under this act are violated may bring a civil action to recover:

actual damages;

statutory damages between $100 and $1,000 per violation;

injunctive or declaratory relief; and

reasonable attorney's fees and costs.

No waiver. Any contract term, arbitration clause, or waiver that purports to limit or waive rights under this section is void and unenforceable.

Sec. 12. [13.912] DATA IMPACT ASSESSMENTS.

Annual assessments. Controllers that engage in data monetization, behavioral profiling, or use automated decision systems with significant effects on individuals must conduct and maintain annual Data Impact Assessments (DIAs).

Contents. DIAs must evaluate:

risks to privacy, equity, and fairness;

potential discriminatory outcomes;

data security and retention practices; and

safeguards used to mitigate harm.

Regulatory access. DIAs must be made available to the Attorney General or the Commissioner of Commerce upon request.

Sec. 13. [13.913] NON-RETALIATION.

A controller or data broker may not deny services, increase prices, degrade quality, or otherwise retaliate against an individual who:

Exercises any right under this act;

Refuses consent for data monetization; or

Requests deletion or correction of personal data.

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

Plain-language explanations. Any automated system used to make or materially assist decisions regarding employment, housing, healthcare, credit, education, or essential services must provide a plain-language explanation describing how personal data is used and the main factors influencing the outcome.

Human appeal. Individuals must be provided a meaningful opportunity for human review of adverse decisions and a channel to contest or appeal such decisions.

Sec. 15. [13.915] RULEMAKING AUTHORITY.

The Commissioner of Commerce may adopt rules necessary to implement this act, including standards for secure data handling, consent disclosures, data broker registration, algorithmic accountability reporting, and calculation of fair compensation.

Sec. 16. [13.916] EFFECTIVE DATE.

This act is effective January 1, 2026, and applies to personal data collected, processed, or monetized on or after that date.