THE DATA DISTRIBUTION FAIRNESS ACT (DDFA)

Minnesota Public Advocacy Draft — 2025

Section 1. SHORT TITLE.

This Act may be cited as the " Data Distribution Fairness Act."

Section 2. PURPOSE AND FINDINGS.

(a) The legislature finds that personal data has measurable economic value and that Minnesotans have no statutory right to transparency, consent, or economic participation regarding its use.

(b) The purpose of this Act is to establish enforceable digital rights, mandate transparent data governance, prohibit exploitative data practices, and ensure individuals share in the economic value their data generates.

Section 3. DEFINITIONS.

(a) " Personal data" means any information relating to an identified or identifiable individual, including derived, inferred, or behavioral data.

(b) " Sensitive data" means data relating to race, health, biometrics, precise location, minors, or financial identity.

(c) " Data broker" means any entity whose primary business is collecting, aggregating, selling, licensing, or otherwise distributing personal data.

(d) " Profiling" means automated processing to evaluate personal preferences, behaviors, creditworthiness, or eligibility for opportunities.

(e) " Monetization" means any revenue-generating use of personal data.

Section 4. INDIVIDUAL RIGHTS.

Individuals have the following rights:

(1) Transparency regarding what personal data is collected, used, and why.

(2) Access to their own personal data.

(3) Correction or deletion of inaccurate or outdated personal data.

(4) Opt – in consent for any monetization or secondary use.

(5) Revocation of consent at any time.

(6) Fair economic participation when personal data is monetized.

Section 5. LIMITATIONS ON DATA COLLECTION AND USE.

(a) Data collection must be limited to what is reasonably necessary for the disclosed purpose.

(b) Data may not be retained longer than necessary.

(c) Dark – pattern consent mechanisms are prohibited.

(d) Personal data collected for one purpose may not be used for incompatible secondary purposes without explicit opt – in consent.

Section 6. DATA MONETIZATION AND COMPENSATION.

(a) No entity may monetize personal data without documented opt – in consent.

(b) Individuals whose data contributes to revenue – generating products or services are entitled to proportional economic compensation.

(c) Compensation models must be disclosed in clear, plain language.

(d) Data brokers must maintain transparent accounting of monetized datasets.

Section 7. PROFILING AND ALGORITHMIC ACCOUNTABILITY.

(a) Automated decisions that significantly affect individuals must include a right to explanation and human review.

(b) Harmful or discriminatory profiling is prohibited.

(c) Entities deploying automated systems must document risk assessments and fairness safeguards.

Section 8. DATA BROKER REGISTRATION.

(a) All data brokers operating in Mnnesota must register annually with the state.

(b) Registration must disclose data sources, uses, and monetization practices.

(c) Failure to register constitutes a violation enforceable by civil penalty.

Section 9. SECURITY AND BREACH NOTIFICATION.

(a) Entities must implement reasonable security measures proportional to the sensitivity of the data.

(b) Data breaches must be disclosed to affected individuals within 72 hours.

(c) Entities failing to maintain adequate safeguards are liable for damages and penalties.

Section 10. ENFORCEMENT.

(a) Attorney General Authority. The Attorney General may investigate violations of this Act, issue civil investigative demands, require the production of documents, compel testimony, and bring civil actions to enforce compliance.

(b) Civil Penalties. Businesses that violate this Act are subject to civil penalties of: (1) up to $7,500 per violation involving personal data; (2) up to $15,000 per violation involving minors or sensitive data.

(c) Injunctive Relief. Courts may issue temporary, preliminary, or permanent injunctions to prevent ongoing or future violations.

(d) Cure Period. For first-time violations, regulated entities have 30 days to cure violations upon receiving notice, unless the violation involves intentional misconduct or the monetization of minors' data.

Section 11. PRIVATE RIGHT OF ACTION.

(a) A Minnesota resident whose rights under this Act are violated may bring a civil action to recover: (1) actual damages; (2) statutory damages between $100 and $1,000 per violation; (3) injunctive or declaratory relief; (4) reasonable attorney's fees.

(b) Arbitration clauses or waivers of rights under this section are void and unenforceable.

Section 12. DATA IMPACT ASSESSMENTS.

(a) Any business engaging in data monetization, behavioral profiling, or automated decision systems must conduct and maintain annual Data Impact Assessments (DIA) that evaluate risks to privacy, equity, and fairness.

(b) DIAs must be made available to the Attorney General upon request.

Section 13. PROHIBITION ON RETALIATION.

A business may not deny services, increase prices, degrade quality, or retaliate against an individual who exercises rights under this Act.

Section 14. TRANSPARENCY IN ALGORITHMIC SYSTEMS.

(a) Any automated system used for employment, housing, healthcare, credit, or essential services must provide plain-language explanations describing how personal data is used.

(b) Individuals must be given a meaningful opportunity for human review of adverse decisions.

Section 15. RULEMAKING AUTHORITY.

The Commissioner of Commerce may adopt rules necessary to implement this Act, including secure data handling standards and algorithmic accountability reporting.

Section 16. EFFECTIVE DATE.

This Act is effective January 1, 2026.