🟥 NEVADA INDIVIDUAL DATA DEFENSE ACT (NIDDA)

AN ACT

Relating to privacy rights and digital protection of Nevada residents; prohibiting the unauthorized sale, sharing, or surveillance of personal, biometric, or behavioral data by public agencies and affiliated contractors; establishing the right to opt out of data collection and to request deletion of state-held data; requiring transparency in all government data-sharing contracts; providing penalties; and providing other matters properly relating thereto.

THE PEOPLE OF THE STATE OF NEVADA DO ENACT AS FOLLOWS:

Section 1. Short Title

This Act shall be known and may be cited as the **Nevada Individual Data Defense Act (NIDDA).**

Section 2. Purpose

To safeguard the digital, biometric, and behavioral data of all Nevada residents by regulating the data practices of public agencies and their contractors; to establish informed consent rights; to guarantee data deletion rights; and to ensure public transparency in all data-sharing contracts and surveillance practices.

Section 3. Definitions

As used in this Act:

1. **"Personal Data"** means any information that identifies, relates to, describes, or could reasonably be linked to a specific person, including but not limited to name, address, email, biometric data, health information, location data, behavioral profiles, or political

affiliations.

2. **"Biometric Data"** includes facial recognition, fingerprint scans, voiceprints, retina scans, gait analysis, and other unique biological identifiers.

3. **"State Entity"** means any department, agency, board, bureau, commission, school district, political subdivision, or public employee acting in official capacity.

4. **"Contractor"** means any person, corporation, nonprofit, or other entity that contracts with a state entity for services or data-processing functions.

5. **"Informed Consent"** means clear, written consent given after full disclosure of how data will be collected, stored, used, shared, or sold.

Section 4. Prohibited Conduct

1. No state entity or contractor shall collect, sell, transfer, share, or allow access to the personal or biometric data of any Nevada resident without prior **informed consent**.

2. No contractor receiving public funds may:

    - Monetize resident data through resale, analysis, or third-party partnerships;

    - Transfer Nevada resident data to affiliates or outside jurisdictions without disclosure;

    - Combine or cross-analyze datasets to build behavioral profiles without consent.

3. No data collected for educational, governmental, health, or civic services may be repurposed for advertising, political messaging, profiling, or predictive policing.

Section 5. Rights of Nevada Residents

1. **Right to Know:** Any Nevada resident may request a report from any state entity or contractor disclosing what data is held, how it was collected, and whom it has been shared with.

2. **Right to Opt Out:** Any Nevada resident may opt out of any non-essential data collection program or analytic platform operated by or on behalf of the state.

3. **Right to Deletion:** Any Nevada resident may request complete and permanent deletion of their non-essential personal or biometric data held by a public entity or contractor.

Section 6. Transparency Requirements

1. All state contracts involving the use, access, analysis, or storage of Nevada resident data must be posted publicly within 30 calendar days of execution.

2. A **Public Data Sharing Registry** shall be created and maintained by the Secretary of State's office. It must be updated monthly with:

    - Vendor names,
    - Contract values,
    - Types of data accessed,
    - Disclosure of resale, AI training use, or analytics services rendered.

Section 7. Penalties

1. Any state employee, official, or contractor that violates this Act may be:

    - Subject to fines of up to **$100,000 per offense**;
    - Disqualified from future state contracts for up to **10 years**;
    - Referred to the Attorney General for criminal data abuse if applicable.

2. Civil penalties recovered under this section shall be deposited into the **Nevada Data Rights Enforcement Fund**, established hereby to fund public education and enforcement of this Act.

Section 8. Whistleblower Protections

Any individual who reports a violation of this Act shall be protected under Nevada whistleblower statutes and may be entitled to a reward of up to **$25,000** upon verified violation and successful enforcement.

Section 9. Severability

If any provision of this Act is held to be invalid, the remainder of the Act shall remain in full force and effect.

Section 10. Effective Date

This Act shall become effective on **January 1, 2026**.

200-Word Summary of Effect (NIDDA)

This initiative prohibits Nevada government agencies and their contractors from collecting, analyzing, sharing, selling, or transferring personal, biometric, or behavioral data without the informed consent of the Nevada resident involved. It applies to all state agencies, school districts, political subdivisions, and any third-party vendors or consultants they hire. The measure guarantees all residents the right to access their stored data, opt out of non-essential data collection, and request deletion of any non-mandatory data held by state-controlled entities.

The Act also requires full transparency by mandating that all data-sharing contracts involving Nevada resident data be posted publicly within 30 days and tracked in a permanent registry. Contractors receiving public funds may not monetize, resell, or cross-analyze resident data. Civil fines of up to $100,000 per violation may apply, with added criminal penalties for abuse. Whistleblowers may be eligible for rewards. The measure also creates a Nevada Data Rights Enforcement Fund to support public oversight and compliance.

This initiative takes effect January 1, 2026, and seeks to reestablish privacy, transparency, and digital dignity for all Nevadans by restricting the unchecked use and misuse of their personal information by public institutions and affiliated vendors.