118th CONGRESS

1st Session

H.R. _____ / S. _____

Digital Autonomy Transparency & Accountability Act

“D.A.T.A. Act”

A Bill

To establish inalienable ownership, transparency, consent, accountability, and control over personal data; to protect digital likeness; to limit algorithmic harms; and for other purposes.

Table of Contents

Section 1. Short Title

This Act may be cited as the “Digital Autonomy Transparency & Accountability Act” or the “D.A.T.A. Act.”

Section 2. Findings and Declaration of Digital Rights

Congress finds that personal data is intrinsic to autonomy, privacy, and personhood. Individuals have the right to possess, control, and protect their personal data against misuse by public and private actors. The People’s digital rights require statutory guarantees of ownership, transparency, consent, auditability, revocation, and due process.

Section 3. Non■transferable Data Ownership

(a) Ownership. All U.S. citizens are the perpetual, exclusive owners of their personal data. (b) Inalienability. Ownership is non■transferable and may not be sold, waived, or assigned except by inheritance or designated delegation under Section 13. (c) Applicability. Ownership applies regardless of how data was collected or derived, including system■generated or inferred data.

Section 4. Definitions

“Covered Entity”: any public or private entity that collects, uses, stores, processes, transfers, or discloses personal data of U.S. citizens. “Personal Data”: any data that identifies or is linkable to a natural person, including identifiers, biometrics, health, financial, communications, behavioral, metadata, location, derivative and inferred profiles, and future data types. “Consent”: freely given, specific, informed, unambiguous, and revocable permission. “Data Lock”: a status that bars access/use/computation of personal data absent a valid court order. “Likeness”: visual, vocal, biometric, or behavioral representations, captured or synthetic. “Algorithmic Decision■making”: automated or semi■automated profiling, scoring, prediction, or classification.

Section 5. Consent Requirements

(a) Granularity. Consent must be requested and recorded per data category and purpose, naming each recipient. (b) No coercion. Conditioning service on non■essential data surrender is prohibited. (c) Revocability. Consent is revocable at any time; revocation takes immediate effect under Section 9. (d) Recordkeeping. Covered Entities must maintain immutable consent timelines.

Section 6. Use of Likeness & AI Replication

(a) Exclusive rights. Individuals hold exclusive rights over their likeness, voice, signature, avatar, and persona. (b) Prohibitions. Unauthorized synthetic media, voice cloning, or impersonation is unlawful except protected parody with clear labeling. (c) Remedies. Rapid takedown, statutory damages, and criminal penalties for malicious intent.

Section 7. Right to Access, Audit, and Revoke

(a) Access. Individuals may obtain copies of all personal data held, in portable format. (b) Audit. Individuals may obtain complete access logs (who, what, when, purpose). (c) Revoke. Individuals may revoke consent for any purpose, and entities must cease processing accordingly.

Section 8. Consent Interface Standards

(a) Plain■language disclosures of category, purpose, recipient, retention, region. (b) Dark■pattern ban; privacy by default. (c) Machine■readable consent receipts compatible with federal API standards.

Section 9. Digital Lock Right (Fifth■Parallel)

(a) Lock. Any person may lock their personal data. (b) Override. Only a court of competent jurisdiction may order access via warrant or subpoena meeting Section 16 requirements. (c) Enforcement. Locked data may not be processed except as ordered; violations are per■subject offenses.

Section 10. Jurisdiction and Preemption

(a) Coverage. Applies to all Covered Entities handling U.S. citizen data, regardless of location. (b) Floor not ceiling. States may enact stronger protections; conflicts resolve to the stronger right. (c) No contract preemption of rights secured herein.

Section 11. Civil and Criminal Penalties

(a) Civil. Up to $25,000 per person per day per violation; fines payable directly to the affected person(s). (b) Criminal. Willful deception, falsification of logs, or malicious deepfake use: fines and imprisonment up to 5 years; enhanced penalties for repeat offenders. (c) Private right of action with attorneys' fees and injunctive relief.

Section 12. Mandatory Data Disclosure by Collectors

Covered Entities must disclose categories collected, purposes, recipients, retention timelines, geographic storage, legal bases, and use of likeness/biometric data; publish an accessible, machine■readable disclosure and maintain revision history.

Section 13. Data Inheritance Framework

(a) Designation. Individuals may designate an inheritor or delegate via secure, auditable mechanisms. (b) Default. In absence of designation, next■of■kin inherits rights consistent with state estate law. (c) Revocation. Designations are revocable and fully auditable.

Section 14. Oversight Office (DAOO)

Establishes a Data Autonomy Oversight Office to administer registry, publish API standards, coordinate enforcement with FTC and State Attorneys General, maintain compliance guidance, and manage public reporting.

Section 15. National Security & Law Enforcement Limitations

Narrowly tailored exceptions require necessity, proportionality, and minimization; no bulk collection; programmatic use requires public reporting to Congress and DAO Office with classified annex where needed.

Section 16. Warrant Standards

Access to locked data requires particularized probable cause, minimization, and time limits; neutral magistrate review; auditable court order identifiers for verification.

Section 17. Irrevocability of Data Ownership

No statute or regulation may redefine data ownership or dilute the rights herein without supermajority assent of the People as provided by constitutional process; ownership remains non■transferable.

Section 18. Cross■Agency Coordination and Harmonization

DAOO shall harmonize this Act with HIPAA, GLBA, FCRA, FERPA, COPPA, CCPA/CPRA analogues, and international frameworks; conflicts resolve to stronger individual rights.

Section 19. Global Enforcement and Reciprocity

Foreign entities handling U.S. citizen data are bound by this Act when doing business in the U.S.; State Department shall pursue reciprocity and treaty alignment; cross■border transfers must preserve rights and auditability.

Section 20. Legal Definitions & Interpretations

Terms shall be construed broadly to maximize protection of individuals; severability applies to all provisions; implementing regulations may refine definitions consistent with the Act’s purposes.

Section 21. Effective Date & Severability

Sections 11, 12, 14, and 16 take effect 180 days after enactment; remaining sections take effect one year after enactment. If any provision is invalidated, the remainder remains in force.