DRAFT LEGISLATION

Personal Data Trusteeship Act

PDTA

An Act to Establish a Trusteeship Framework for Personal Data, Enhance Individual Control Over Sensitive Information, and Protect Liberty and Autonomy in the Digital Age *Companion statute to the Verifiable Identity and Digital Autonomy Act (VIDA) and the Government Algorithmic Accountability and AI Fiduciary Act (GAAFA)*

Prepared by Michael G. Leahy

Initial Draft | March 2026

Be it enacted by the [Legislative Body] as follows:

Section 1. Short Title

(a) This Act may be cited as the "Personal Data Trusteeship Act" or the "PDTA."

Section 2. Findings and Purpose

(a) Findings

The [Legislative Body] finds that:

(1) Personal and sensitive data, including personally identifiable information, constitutes a commons of unownable facts under established legal principles, including copyright law, where protection extends only to database compilations and not to the underlying facts themselves.

(2) Traditional ownership models for data lead to commodification, monopolistic control, and inequities, stifling innovation and equitable access while exacerbating power imbalances between individuals and data collectors, processors, and sharers.

(3) A trusteeship model, wherein individuals serve as primary trustees over their own data, aligns with fiduciary principles from trust law, promoting accuracy, timeliness, and controlled use without proprietary exclusion.

(4) Governments bear an enhanced fiduciary duty of loyalty and care in protecting natural persons' liberty and autonomy from data-related harms, as articulated in scholarship emphasizing relational protections against opportunism in data handling.

(5) Power disparities between individuals and data-handling entities necessitate mechanisms that favor individuals, including private rights of action and accessible remedies, to counter exploitation by entities with superior resources and information.

(6) Existing privacy frameworks, while valuable, require supplementation with fiduciary duties to address trust gaps and ensure proactive safeguards for personal autonomy in an era of pervasive data collection and AI-driven processing.

(7) The Fourth Amendment's particularity requirement, applied to the digital context, prohibits government from maintaining data systems of perpetual duration, universal scope, and discretionary access that are the functional equivalent of the general warrants condemned by the Founders.

(8) Citizens can have no meaningful autonomy when the government holds comprehensive, aggregated records of their activities, associations, beliefs, and movements in systems accessible to broad classes of officials without individualized justification.

(9) In addition to the Fourth Amendment grounding recited in subsection (7), the Constitution of [Enacting State] independently grounds the duties established by this Act. [Citation to State's popular-sovereignty or social-compact clause], which vests political power in the people and establishes government for their protection and benefit, establishes the fiduciary relationship between government and the individual as a matter of state constitutional structure, independent of this Act's statutory text.

(10) [Citation to State's inherent-rights clause], which secures to persons rights held independent of and prior to any grant from the state, establishes that an individual's identity, and the personal data constituting it, is not property the state originated or owns. Government that takes custody of an individual's identity attributes holds something belonging to another.

(11) [Citation to State's search-and-seizure clause], [brief parenthetical description of its particularity, reasonableness, and warrant structure], independently establishes the four fiduciary duties of loyalty, care, confidentiality, and transparency recited in subsection (7), without reliance on federal Fourth Amendment doctrine and without regard to future changes in that doctrine.

(12) [Where the enacting state's constitution contains such a clause: citation to a fundamental-principles or reserved-rights clause] instructs that recurrence to fundamental principles is essential to the security of individual rights. This Act's findings under subsections (9) through (11) shall be construed together as an integrated statement of [Enacting State]'s constitutional structure, not as separate and unrelated provisions.

(b) Purpose

The purpose of this Act is to:

(1) Establish individuals as primary trustees over their personal data, empowering them with authority to manage, control, access, correct, and delete their data;

(2) Impose fiduciary obligations on all entities that handle personal data, with enhanced duties on government emphasizing loyalty and care to protect individual liberty;

(3) Provide private rights of action and effective remedies to enable individuals to enforce their rights without dependence on government enforcement discretion;

(4) Foster a balanced data ecosystem that treats personal facts as a commons, promoting innovation while mitigating harms from aggregation, profiling, and surveillance;

(5) Establish the bilateral trust structure within which government may operate as a limited secondary fiduciary, authorized to endorse or verify factual claims without creating centralized identity repositories; and

(6) Create the legal superstructure that, together with the technical architecture of VIDA and the AI governance provisions of GAAFA, forms a complete constitutional framework for government's digital relationship with citizens.

Section 3. Definitions

For the purposes of this Act, the following terms have the meanings indicated. Capitalized terms defined in VIDA or GAAFA have the same meanings as in those Acts unless this Act provides otherwise.

(a) "Personal Data" means any information relating to an identified or identifiable natural person, including personally identifiable information (PII) and sensitive data such as health, financial, biometric, or location information.

(b) "Data Subject Trustee" means the natural person to whom the personal data relates, designated as the primary trustee with fiduciary authority over such data.

(c) "Secondary Fiduciary" means any entity, including collectors, processors, sharers, or government agencies, that handles personal data on behalf of or in relation to the data subject trustee. For purposes of this Act and GAAFA, Secondary Fiduciary includes autonomous AI agents deployed by government agencies to query, process, or act upon personal data.

(d) "Fiduciary Duties" include the duty of loyalty (acting in the best interests of the data subject without opportunism), the duty of care (exercising reasonable efforts to protect and manage data accurately and securely), the duty of confidentiality (refraining from unauthorized disclosure, sale, or secondary use of personal data), and the duty of impartiality (fair handling without undue influence from conflicting interests).

(e) "Data Commons" refers to the treatment of underlying personal facts as unownable public resources, subject to trusteeship rather than proprietary rights.

(f) "Government Entity" includes any state, county, or local agency, department, board, commission, authority, or instrumentality involved in data handling, regulation, or the provision of public services.

(g) "Data Trusteeship Authority" or "DTA" means the government body established by Section 7(b)(3) of this Act to oversee compliance, conduct audits, and enforce the standards of this Act.

(h) "Immutable Audit Trail" means a tamper-evident, append-only electronic record of all data interactions, transactions, and access events related to a citizen's personal data, accessible by the citizen through a secure, individually controlled portal.

(i) "VIDA" means the Verifiable Identity and Digital Autonomy Act, and references to specific sections of VIDA refer to the sections of that Act as enacted and subsequently amended.

(j) "GAAFA" means the Government Algorithmic Accountability and AI Fiduciary Act, and references to specific sections of GAAFA refer to the sections of that Act as enacted and subsequently amended.

Section 4. Establishment of Personal Data Trusteeship

Cross-references: VIDA Sec. 7(a)(1) (Holder Control: individuals retain exclusive control over credentials via personal digital wallet); VIDA Sec. 7(a)(13) (Rights of individuals to control digital identity)

(a) Every natural person is hereby designated as the primary trustee over their own personal data, with overriding authority to manage, access, correct, and control its use. This trusteeship is inalienable and may not be waived, contracted away, or extinguished by any government action or private agreement.

(b) Personal data shall be treated as a commons, ineligible for ownership claims, with any database protections limited to structural compilations and not extending to the underlying facts themselves.

(c) Secondary fiduciaries must obtain explicit, revocable authorization from the data subject trustee for any collection, processing, or sharing of personal data. Authorization shall be specific to the stated purpose and shall be subject to automated tools for real-time oversight, including the secure individual-controlled portal required by Section 6A(c) of this Act.

(d) The primary trusteeship established by this section shall be superior to and shall not be diminished by any contract, terms of service, consent form, or other agreement that purports to transfer, waive, or limit the trustee's rights over their personal data.

Section 4A. Bilateral Trust Structure

Cross-references: VIDA Sec. 3A (Prohibition on Surveillance Architectures); VIDA Sec. 7(a)(12) (Preference for Endorsement over Issuance); VIDA Sec. 8 (Data Minimization and Sequestered Databases); GAAFA Sec. 4 (Constitutional and Fiduciary Foundations)

(a) Individuals shall act as primary trustees over their personal data, holding stewardship responsibilities for accuracy, timeliness, and civic participation, while retaining inalienable autonomy rights that no government action may diminish.

(b) Government entities shall serve as limited secondary fiduciaries, authorized only to endorse or verify factual claims (including age, residency, licensure, and other legally relevant attributes) without creating or maintaining centralized identity repositories. Endorsement shall use cryptographic methods, including verifiable credentials and zero-knowledge proofs, to ensure verifiability without data retention, consistent with VIDA Section 7(a)(12)'s preference for government endorsement over government issuance.

(c) Secondary fiduciaries, including government entities, shall not repurpose data beyond the original justified purpose without fresh, explicit authorization from the data subject trustee. This prohibition is traceable directly to the Fourth Amendment's particularity requirement, which demands that government justify each intrusion on individual data by reference to a specific, articulated need. Repurposing without fresh authorization violates the loyalty duty and constitutes a per se breach of this Act.

(d) The bilateral trust structure established by this section defines the outer limits of lawful government data conduct. A government entity that holds citizen data as a secondary fiduciary may not use that status to build the surveillance capability that VIDA Section 3A prohibits. The fiduciary role entitles government to hold data for the specific purpose for which it was collected; it does not entitle government to aggregate, cross-reference, profile, or retain data beyond that purpose.

Section 4B. Fiduciary relationship arising from collection

Cross-references: PDTA Sec. 4 (Establishment of Personal Data Trusteeship); PDTA Sec. 4A (Bilateral Trust Structure); VIDA Sec. 3B (Identity association as participatory act)

(a) The fiduciary relationship established by this Act arises at the moment of data collection, not at the moment of any subsequent consent interaction, terms-of-service agreement, or contractual authorization. Any entity that collects personal data about an identifiable individual in connection with a government function assumes the duties of a secondary fiduciary under Section 6 of this Act from the moment of collection, regardless of whether the individual has agreed to any terms, clicked any button, or entered any contractual relationship with the collecting entity.

(b) For purposes of this section, "in connection with a government function" includes:

(1) Direct collection by a government entity;

(2) Collection by a vendor, contractor, or subcontractor performing services under a government contract, grant, or cooperative agreement;

(3) Collection by any entity that subsequently sells, licenses, shares, or otherwise provides personal data to a government entity; and

(4) Collection by any entity operating identity verification, benefits administration, licensing, regulatory compliance, or other systems on behalf of a government entity.

(c) The fiduciary duties established by this Act may not be disclaimed, limited, or conditioned by any click-through agreement, terms of service, privacy policy, consent form, or other instrument of adhesion. A secondary fiduciary may not condition the provision of government services, or services provided in connection with a government function, on an individual's acceptance of terms that purport to waive, limit, or modify the fiduciary protections of this Act.

(d) This section does not impose fiduciary duties on commercial entities acting outside any government connection. The regulation of purely commercial data

collection is addressed by the Commercial Surveillance and Digital Likeness Protection Act and does not derive from the constitutional fiduciary relationship that grounds this Act.

Section 5. Duties and Rights of Data Subject Trustees

Cross-references: VIDA Sec. 10(a) (Individual rights: access, correction, erasure, portability, private right of action); GAAFA Sec. 6 (Right to Algorithmic Explanation); GAAFA Sec. 8(d) (Citizen access to agentic audit trails)

(a) Duties

Data subject trustees shall exercise fiduciary duties to maintain the accuracy and timeliness of their own personal data to the best of their ability, with support from government-provided tools and resources under Section 7(b)(2) of this Act. The duty of accuracy is a stewardship obligation, not a condition of trustee rights; failure to maintain perfect data accuracy does not diminish a trustee's rights under this Act.

(b) Rights

Trustees have the following rights, enforceable through the private right of action established by Section 8 of this Act:

(1) Access: the right to access comprehensive logs of all data interactions, including all queries, disclosures, and processing events, through the individual-controlled, immutable audit trail required by Section 6A(c);

(2) Veto and Revocation: the right to veto any proposed data use and to revoke any previously granted authorization at any time, with effect within a reasonable time not to exceed [72 hours] of revocation notice;

(3) Correction and Deletion: the right to demand correction of inaccurate data and deletion of data no longer required for the original authorized purpose, with government compliance within [30 days] of demand;

(4) Delegation: the right to delegate limited authority to trusted agents, including legal representatives, advocates, and AI assistants, while retaining ultimate trusteeship and the ability to revoke any delegation;

(5) Portability: the right to receive all personal data held by government entities in a structured, commonly used, and machine-readable format for transfer to another provider or platform, consistent with VIDA Section 4(b)(4)'s duty of portability; and

(6) Explanation: the right to receive an intelligible explanation of any adverse decision made or substantially influenced by an Automated Decision System, as specified in GAAFA Section 6.

(c) Guardianship

For minors, incapacitated individuals, or others temporarily or permanently unable to exercise trusteeship, guardians may be appointed with appropriate court oversight. Guardianship appointments shall:

(1) Ensure that the guardian's decisions align with the ward's best interests and minimize the ward's data exposure;

(2) Be subject to the same fiduciary duties and accountability mechanisms that this Act imposes on secondary fiduciaries;

(3) Be revocable by the ward upon reaching majority or recovering capacity; and

(4) Be consistent with the delegation and guardianship support requirements of VIDA Section 7(a)(4).

Section 6. Obligations of Secondary Fiduciaries

Cross-references: VIDA Sec. 4 (Data Fiduciary Duties); VIDA Sec. 4A (Protections Against AI-Enabled Threats); GAAFA Sec. 4 (Constitutional and Fiduciary Foundations); GAAFA Sec. 8 (Agentic AI as Statutory Secondary Fiduciary); VIDA Sec. 4C (Commercial Duty of Ecosystem Participation)

(a) General Duties. Secondary fiduciaries must adhere to the fiduciary duties of loyalty, care, confidentiality, and impartiality, prioritizing the data subject trustee's interests in all data handling activities. In particular:

(1) Duty of Loyalty: A secondary fiduciary must act in the best interests of the data subject and must not use personal data for any purpose that serves the fiduciary's own interests at the expense of the data subject's interests, including data sharing arrangements, commercial uses, or law enforcement disclosures that the data subject trustee did not authorize;

(2) Duty of Care: A secondary fiduciary must implement appropriate security, transparency, and governance practices to protect the integrity and confidentiality of personal data, including the technical safeguards required by VIDA Section 7(a)(5) (Zero Trust Architecture) and Section 8 (Data Minimization and Sequestered Databases);

(3) Duty of Confidentiality: A secondary fiduciary must refrain from unauthorized disclosure, sale, or secondary use of personal data; and

(4) Duty of Impartiality: A secondary fiduciary must handle personal data without undue influence from conflicting interests, including commercial relationships with data brokers, law enforcement sharing agreements not authorized by the data subject, or cross-agency sharing that exceeds the original collection purpose.

(b) Burden of Proof. In cases of power disparity between a data subject trustee and a secondary fiduciary, including all government-citizen data disputes, the secondary fiduciary bears the burden of demonstrating compliance with the fiduciary duties of this Act. The data subject

trustee is not required to demonstrate the fact of a breach; the secondary fiduciary must affirmatively establish compliance.

(1) Where a government secondary fiduciary asserts the data subject trustee's authorization as a defense to an alleged breach of the duty of loyalty, the government secondary fiduciary bears the burden of establishing, by clear and convincing evidence, that:

(i) the authorization was not a condition of the trustee's receipt of a benefit, license, service, or right; and

(ii) the trustee had a genuine alternative to providing the authorization.

(2) An authorization is not a genuine alternative under paragraph (1)(ii) merely because the trustee could have declined to seek the benefit, license, service, or right in question. The inquiry asks whether the trustee had a practical means of obtaining the specific government function sought without providing the authorization, not whether the trustee could have foregone the function altogether.

(3) This standard does not apply to secondary fiduciaries other than government entities. Vendor secondary fiduciaries remain governed by subsection (d) of this section, which imposes the same standard as paragraphs (1) and (2) on Vendors as a matter of contract. Where an entity is not a Secondary Fiduciary under this Act because it is a Commercial Participant under VIDA rather than a Vendor acting in connection with a government function, its authorizations are instead governed by the express, informed, specific, and revocable consent standard established under VIDA Section 4C(c).

(c) Data Minimization. Secondary fiduciaries shall collect only the minimum personal data necessary for the specific, stated, legally authorized purpose. Collection beyond the minimum, or retention beyond the period necessary for the authorized purpose, constitutes a presumptive breach of the duty of care.

(d) Vendor Obligations. Where a secondary fiduciary retains a Vendor to handle personal data, the secondary fiduciary remains jointly and severally liable for all fiduciary breaches arising from the Vendor's conduct. The secondary fiduciary's contract with the Vendor shall impose the full fiduciary duty regime of this Act on the Vendor and shall provide for the data subject trustee's enforcement rights as a third-party beneficiary of that contract.

Section 6A. Architectural Requirements for Fiduciary Compliance

Cross-references: VIDA Sec. 7(a)(5) (Zero Trust Architecture); VIDA Sec. 8 (Data Minimization and Sequestered Databases); VIDA Sec. 6(a)(2) (Selective disclosure and data minimization); GAAFA Sec. 5 (Algorithmic Deployment Assessment requirements referencing this section); GAAFA Sec. 8(b) (Agentic AI authorization requirements)

The fiduciary duties of this Act cannot be discharged through procedural compliance alone; they require architectural implementation. The following technical requirements establish the minimum architectural baseline for fiduciary compliance.

(a) Purpose-Limited Sequestration. Secondary fiduciaries shall implement purpose-limited sequestration, ensuring that data collected for one purpose (including tax administration, benefits eligibility, licensing, vital records, and law enforcement) is isolated in separate, technically enforced datasets and is not accessible to systems serving different purposes without fresh, explicit authorization from the data subject trustee. Cross-purpose access without fresh authorization is a breach of the duty of loyalty regardless of whether it produces demonstrable harm.

(b) Zero-Knowledge Verification Preference. Where verification of a fact suffices to fulfill a government function, credential-based verification using zero-knowledge proofs, selective disclosure mechanisms, or other cryptographic protocols is the required default. A secondary fiduciary may collect the underlying personal data supporting that fact only upon an affirmative, documented determination, made and recorded before collection, that credential-based verification was not technologically feasible for the specific transaction. The determination shall be recorded in the audit trail required by subsection (c).

(c) Individual-Controlled Immutable Audit Trails. All systems handling personal data under this Act shall maintain individual-controlled, immutable audit trails for all data interactions, including every query, access, disclosure, processing event, and automated decision output. Audit trails shall be:

(1) Accessible by the data subject trustee through a secure individual portal using the same cryptographic authentication infrastructure required by VIDA Section 7(a)(5);

(2) Tamper-evident and append-only, such that no record of a data interaction may be deleted or modified after creation;

(3) Retained for a period sufficient to support enforcement of the data subject's rights, not less than [seven years] from the date of the interaction; and

(4) Extended, pursuant to GAAFA Section 8(c), to include a complete record of all Automated Decision System outputs and agentic AI actions taken in connection with the data subject's data.

(d) Cryptographic Authentication. To counter AI-generated synthetic media and impersonation threats, secondary fiduciaries shall prioritize cryptographic signatures for all authentication, rendering presentation media (including videos, images, and voice recordings) legally irrelevant for identity verification purposes. Systems relying on biometric presentation without cryptographic verification of underlying credentials do not satisfy the authentication requirements of this Act, consistent with VIDA Section 4A(a)'s requirement for zero-knowledge proofs and cryptographic signatures.

Section 6B. Prohibition on government acquisition of commercially compiled surveillance data

Cross-references: PDTA Sec. 6 (Obligations of Secondary Fiduciaries); VIDA Sec. 3A (Prohibition on Surveillance Architectures); VIDA Sec. 4B (Digital likeness and synthetic identity protections)

(a) No government entity, and no entity acting on behalf of or in connection with a government function, shall purchase, license, receive, or otherwise acquire personal data, compiled behavioral profiles, location data, biometric data, browser tracking data, or any data derived from commercial surveillance activities, except pursuant to:

(1) A valid warrant supported by probable cause, satisfying the particularity requirement of the Fourth Amendment, and specifically identifying the individual whose data is sought and the data elements to be obtained; or

(2) A lawful subpoena or court order issued in connection with a specific, identified legal proceeding or investigation, subject to the data minimization requirements of Section 6A(b) of this Act.

(b) For purposes of this section, "commercial surveillance activities" means any collection, compilation, correlation, or analysis of personal data about identifiable individuals conducted by a non-government entity for commercial purposes, including but not limited to:

(1) Browser fingerprinting and cross-site tracking;

(2) Location data collection through mobile applications, cellular infrastructure, or connected devices;

(3) Behavioral profiling for advertising, marketing, or analytics purposes;

(4) Data brokerage, meaning the aggregation and sale of personal data from multiple sources; and

(5) Algorithmic inference of personal attributes from behavioral data.

(c) The prohibition in this section applies regardless of whether the data has been anonymized, de-identified, aggregated, or otherwise processed, if the data can be re-identified or associated with a specific individual through any technically feasible means.

(d) A government entity that acquires commercially compiled data in violation of this section is subject to the enforcement provisions of Section 8 of this Act. Data acquired in violation of this section is inadmissible in any judicial, administrative, or regulatory proceeding, and any derivative evidence obtained through use of such data is subject to suppression.

(e) The duty of accounting established by Section 6(a) of this Act includes, for any secondary fiduciary that derives commercial revenue from compiled personal data profiles: the obligation to disclose, upon request by the data subject trustee, what personal data was collected, what commercial value was derived from compilation or analysis of that data, how that value was distributed, and what portion, if any, was returned to or for the benefit of the data subject.

Section 6C. Presumptively Disloyal Practices

Cross-references: PDTA Sec. 3(c) (Secondary Fiduciary); PDTA Sec. 6(a) (General Duties); PDTA Sec. 6(b) (Burden of Proof, including the consent-rebuttal standard); PDTA Sec. 6(d) (Vendor Obligations); PDTA Sec. 6A (Architectural Requirements for Fiduciary Compliance); PDTA Sec. 8 (Private Rights of Action)

(a) A practice or activity described in this section is a presumptive violation of the duties established by Section 6(a). It is a presumptively disloyal practice for a secondary fiduciary to:

(1) process, use, or share personal data for any purpose other than the specific, stated, legally authorized purpose for which it was collected, without authorization meeting the standard of Section 6(b)(1);

(2) link or correlate personal data, or a record of a data interaction, with personal data or behavioral data collected in an unrelated interaction or context;

(3) disclose personal data to a private-sector actor absent independent legal authorization or authorization meeting the standard of Section 6(b)(1);

(4) collect or request personal data beyond the minimum necessary for the specific, stated purpose, in violation of Section 6(c);

(5) retain personal data beyond the period reasonably necessary for the specific, stated purpose, absent an independent legal retention obligation;

(6) fail to delete or de-identify personal data upon completion of the stated purpose or upon the data subject trustee's request, absent an independent retention obligation;

(7) collect an underlying personal data element without the affirmative, documented, pre-collection determination required by Section 6A(b);

(8) fail to maintain technical and administrative safeguards commensurate with the sensitivity of the personal data held, notwithstanding the requirements of Section 6A;

(9) permit access to stored personal data by personnel, an employee, a contractor, or an agent for a purpose other than the specific, stated purpose, without independent authorization;

(10) deny a data subject trustee's request to access, obtain a copy of, or correct the personal data held about that trustee; or

(11) fail to maintain or provide, upon request, a record of processing and disclosure sufficient for the data subject trustee to verify the secondary fiduciary's compliance with this Act.

(b) The presumption established by subsection (a) is rebutted:

(1) for paragraph (7), by production of the affirmative, documented, pre-collection determination required by Section 6A(b); and

(2) for all other paragraphs of subsection (a), only by clear and convincing evidence meeting the requirements of Section 6(b)(1) through (3).

Section 7. Government Duties

Cross-references: VIDA Sec. 2 (Legislative Findings and Purpose); VIDA Sec. 4 (Data Fiduciary Duties); VIDA Sec. 10(c) (Data Fiduciary Oversight Office); GAAFA Sec. 10 (Technical AI Oversight Capacity, which amends this section)

(a) Enhanced Fiduciary Role

Government entities shall act as overarching fiduciaries in data governance, with enhanced duties of loyalty and care to protect natural persons' liberty and autonomy from data-related threats, including surveillance, manipulation, exploitation, and the harms that arise from AI-mediated government decisions. Government's fiduciary role includes preventing opportunism in data use and addressing trust gaps through relational protections that go beyond consent-based models. A government entity that uses citizen data to build surveillance capability, generate behavioral profiles, or share information with other agencies or private parties beyond the original collection purpose has violated its loyalty duty regardless of whether the data subject consented to the original collection.

(b) Specific Obligations

Governments must:

(1) Favor individuals in disputes involving significant power imbalances, applying a presumption of validity to trustee claims and shifting evidentiary burdens to secondary fiduciaries or government actors in all administrative and judicial proceedings under this Act;

(2) Provide free or subsidized resources, including legal aid, technological tools (including data dashboards, access portals, and AI assistants that help individuals exercise their trustee rights), and education programs, to enable effective trusteeship by individuals who lack the resources and technical expertise to navigate data governance systems independently;

(3) Establish a Data Trusteeship Authority (DTA) to oversee compliance, conduct audits, and enforce the standards of this Act, with authority to:

(i) Investigate complaints filed by data subject trustees against secondary fiduciaries;

(ii) Impose civil penalties up to [specified amounts] for violations of this Act;

(iii) Order remediation, including data deletion, access revocation, cessation of processing, and system modifications;

(iv) Conduct proactive audits of secondary fiduciaries, including government agencies, without requiring a complaint; and

(v) Fulfill the AI-specific functions assigned to the DTA by GAAFA Section 10(b);

(4) Prohibit government use of personal data for purposes that undermine autonomy, including unwarranted surveillance, and require impact assessments for any data initiative that collects, processes, or retains personal data beyond what is minimally necessary for a specific, legally authorized purpose, consistent with GAAFA Section 9's Algorithmic Impact Assessment requirements;

(5) Promote legislative and regulatory reforms to integrate data loyalty principles, ensuring protections against emotional data misuse, facial recognition abuses, and other emerging threats to liberty, including the AI governance reforms addressed by GAAFA; and

(6) Collaborate internationally to harmonize standards, recognizing the global nature of data flows while prioritizing domestic safeguards for individual autonomy.

(c) Accountability

Government breaches of the duties established by this section shall trigger heightened scrutiny in any judicial or administrative proceeding, with remedies favoring restoration of individual control and compensation for harms to liberty. The burden of demonstrating compliance in any proceeding under this Act rests on the government entity, not on the data subject trustee.

Section 8. Private Rights of Action

Cross-references: VIDA Sec. 10(a)(5) (Private right of action for violations of VIDA); GAAFA Sec. 11 (Enforcement, incorporating this section's private right of action)

(a) Any data subject trustee may bring a civil action in [appropriate court] against any secondary fiduciary or government entity for violations of this Act, including breaches of fiduciary duties, unauthorized data handling, failures to honor trustee rights, and violations of the architectural requirements of Section 6A. Actions may be brought individually or collectively as class actions.

(b) No pre-dispute arbitration clauses or class action waivers shall apply to actions under this Act. Any contractual provision purporting to waive the right to bring an action under this Act, or to require arbitration of claims arising under this Act, is void and unenforceable as against public policy.

(c) Actions may be filed without prior administrative exhaustion. The statute of limitations for actions under this Act is [five years] from the later of: (1) the date of the violation; or (2) the date the data subject trustee discovered or reasonably should have discovered the violation. For violations involving concealed data collection or undisclosed secondary use, the discovery rule tolls the limitations period until the trustee had or reasonably should have had actual knowledge of the violation.

(d) Where the same conduct constitutes a violation of both this Act and VIDA or GAAFA, the plaintiff may assert all available claims in a single action. The private right of action under this Act is cumulative and does not supersede or limit any right of action available under VIDA, GAAFA, or any other provision of law.

Section 9. Remedies

Cross-references: GAAFA Sec. 11(c) (Remedies in GAAFA enforcement actions, incorporating this section by reference)

(a) Available Remedies

Courts may award in actions under this Act:

(1) Injunctive relief, including data deletion, access revocation, cessation of processing, modification of data handling systems, and mandamus to compel compliance with the requirements of this Act;

(2) Compensatory damages for actual harms, including economic losses, denial of benefits or services to which the trustee was entitled, and harm from liberty infringements including surveillance, profiling, and discriminatory automated decisions;

(3) Statutory damages of [not less than $1,000 per violation], scalable based on willfulness, duration, and the number of individuals affected;

(4) Punitive damages for egregious breaches of loyalty or care, including deliberate data repurposing, knowing maintenance of non-compliant surveillance architectures, and willful failure to respond to trustee demands for access or correction; and

(5) Attorneys' fees and costs to prevailing plaintiffs.

(b) Equitable Access

To address resource disparities between data subject trustees and secondary fiduciaries, courts shall:

(1) Provide expedited procedures for emergency injunctive relief in cases involving ongoing data collection, processing, or surveillance;

(2) Waive filing fees for low-income trustees upon sworn showing of financial need; and

(3) Apply a presumption in favor of class certification where the plaintiff establishes that a secondary fiduciary's breach affected or is likely to have affected multiple data subject trustees through the same system, policy, or practice.

(c) Government-Specific Remedies

For government violations, remedies include:

(1) Mandamus to compel compliance with specific provisions of this Act;

(2) Sovereign immunity waived for monetary awards up to [specified limits], paid from the operating budget of the responsible agency and not from the general fund, consistent with VIDA Section 4(d)(3); and

(3) Prohibition on indemnification of officers or employees found to have committed willful or knowing violations of this Act using public funds, consistent with VIDA Section 4(d)(4).

Section 10. Enforcement

Cross-references: VIDA Sec. 10(d) (Attorney General enforcement authority); GAAFA Sec. 10(b) (Amendment of DTA to include AI-specific mandates); GAAFA Sec. 11(e) (Attorney General enforcement authority under GAAFA)

(a) The Data Trusteeship Authority shall have primary enforcement authority under this Act, with powers to:

(1) Investigate complaints and conduct proactive audits without requiring a prior complaint;

(2) Issue subpoenas for documents, data, and testimony;

(3) Impose civil penalties up to [specified amounts] for violations of this Act;

(4) Issue cease-and-desist orders, remediation orders, and orders requiring system modifications; and

(5) Refer matters to the Attorney General for criminal prosecution where violations are willful and egregious.

(b) The DTA shall coordinate with existing enforcement agencies, including the [state consumer protection authority] and relevant federal agencies, integrating PDTA principles into broader privacy enforcement activities.

(c) The DTA shall submit annual reports to [the Legislative Body] on compliance levels across government and private secondary fiduciaries, emerging data threats, enforcement actions taken, and recommendations for legislative updates. AI-specific reporting requirements are addressed in GAAFA Section 10(b)(4).

Section 11. Severability

(a) If any provision of this Act or its application to any person or circumstance is held invalid or unenforceable, the remainder of this Act and the application of its provisions to other persons or circumstances shall not be affected and shall continue in full force and effect.

Section 12. Effective Date

(a) This Act shall take effect [180] days after enactment.

Section 13. Cross-Referencing and Statutory Construction

(a) This Act shall be construed in harmony with the Verifiable Identity and Digital Autonomy Act (VIDA) and the Government Algorithmic Accountability and AI Fiduciary Act (GAAFA) to create a comprehensive and integrated framework for constitutional digital governance. PDTA provides the legal superstructure of fiduciary duties; VIDA provides the technical architecture within which those duties are discharged; GAAFA governs the use of AI within that architecture

and under those obligations. Where this Act and VIDA or GAAFA address the same subject matter, the provision that provides greater protection to the data subject trustee shall govern.

(b) This Act does not limit any right or remedy available to a citizen under VIDA, GAAFA, the Fourth Amendment to the United States Constitution, the equal protection guarantees of the state and federal constitutions, applicable civil rights statutes, or any other provision of law. The rights and remedies provided by this Act are cumulative and in addition to all other rights and remedies.

Section 14. Sunset Review

(a) The Data Trusteeship Authority, in coordination with the Data Fiduciary Oversight Office established by VIDA Section 10(c), shall review this Act and report to [the Legislative Body] on its implementation, effectiveness, and recommended amendments every [5] years following the effective date. The review shall specifically assess whether the bilateral trust structure of Section 4A remains an adequate constraint on government data aggregation given developments in technology, whether new categories of secondary fiduciary require additional provisions, and whether the integration of this Act with VIDA and GAAFA requires updating.

Section 15. Funding and Resources

(a) The [state agency] shall allocate funds from [source] to support implementation of this Act, including:

(1) Establishment and staffing of the Data Trusteeship Authority;

(2) Development of the individual-controlled audit trail portals required by Section 6A(c);

(3) Public education campaigns explaining the rights and remedies available under this Act;

(4) Legal aid and technological tool development for low-income, low-digital-literacy, and underserved populations; and

(5) Coordination with VIDA implementation funding under VIDA Section 17 and GAAFA implementation funding under GAAFA Section 13(f) to avoid duplication and maximize efficiencies.

About this Draft

This is an initial formatted draft of the Personal Data Trusteeship Act (PDTA), prepared as a companion statute to the Verifiable Identity and Digital Autonomy Act (VIDA) and the Government Algorithmic Accountability and AI Fiduciary Act (GAAFA). All bracketed provisions indicate items requiring legislative specification. Cross-references to VIDA and GAAFA reflect the section numbering of the March 2026 drafts of those Acts. This draft is prepared for discussion and does not represent the position of any government body.