Initiative 2025-2026 #271
Digital Property and Data Rights

Received by Legislative Council Staff
3/6/26 at 5:21 AM

STATE OF COLORADO

BILL 1

PERSONAL DATA AND DIGITAL PROPERTY RIGHTS ACT

A Bill for an Act Concerning the Establishment of Resident Digital Data as Inalienable Intangible Personal Property, the Resident Data Registry, the Master Data Settlement and Restitution Agreement, and Physical Access Infrastructure for Digital Rights Enforcement

AMPLIFY Act — Bill 1 of 3 | Title 15, Article 15 | AMPLIFY Act

ENACTING CLAUSE & SINGLE SUBJECT

Be it Enacted by the People of the State of Colorado:

Single subject. This act concerns the establishment and enforcement of resident digital property rights, including the definition and protection of The Digital Soul as inalienable intangible personal property, the Master Deed registry system, Audit Marker enforcement architecture, the Master Data Settlement and Restitution Agreement mechanism, analog bridge infrastructure, spousal veto power, and a directive to the General Assembly to refer a constitutional amendment enshrining The Digital Soul.

SECTION 1. LEGISLATIVE DECLARATION

(1) The general assembly finds and declares that: (a) The Digital Soul — encompassing biometric data, behavioral data, derived biological data, civic telemetry, and all emergent automation-generated inferences derived therefrom — constitutes an inalienable intangible personal property right of every Colorado resident, co-equal in dignity and enforceability with tangible personal property; (b) The unauthorized extraction, scraping, ingestion, training upon, or commercial monetization of The Digital Soul constitutes a severance event and a taking of private property requiring just compensation; (c) A state Master Deed registry, resident-controlled Resident Automated Mitigation Accounts, and a non-circumventable analog bridge infrastructure are necessary to give residents full, practical enjoyment of their digital property rights; (d) Historical violations of resident digital property rights by covered operators require an aggressive enforcement mechanism — the Master Data Settlement and Restitution Agreement 'Legacy Use Settlement Program' — leveraging existing attorney general powers augmented by new statutory damages; and (e) The rights established in this article are so fundamental to resident sovereignty that the General Assembly shall refer a constitutional amendment to the voters of Colorado to permanently enshrine The Digital Soul as inalienable intangible personal property under the Colorado Constitution.

MSSA DISQUALIFICATION. ***Severe violations; loss of settlement protections; forfeiture.***
(1) Grounds. A signatory operator is subject to disqualification from participation in the Master Settlement and Settlement Agreement program (MSSA) upon a finding of a severe violation, including: (a) knowing or reckless circumvention of the registry, Audit Markers, or Trust safeguards; (b) material misrepresentation in reporting, auditing, or certification; (c) repeated unauthorized ingestion, training, or use after notice; (d) retaliation against a resident exercising rights under this article; or (e) any other egregious noncompliance defined by rule that presents substantial risk of harm.
(2) Procedure; due process. Disqualification may occur only after notice, an opportunity to be heard, and a written determination by the administrator, subject to administrative appeal and judicial review as provided by law. The administrator may impose interim measures necessary to prevent imminent harm pending a final determination.
(3) Effect of disqualification; litigation exposure restored. Upon final disqualification, any release, safe harbor, reduced-liability schedule, or other benefit of MSSA participation is void as to the disqualified operator for the period of noncompliance, and the state and residents may pursue any otherwise available administrative, civil, or criminal remedies, including claims that would have been released or limited by MSSA participation, to the extent permitted by law.
(4) Forfeiture; no refund. Amounts previously paid by the disqualified operator into MSSA-related funds, mitigation pools, or resident payment mechanisms are forfeited to the program and shall not be refunded or credited back to the operator. The administrator may apply forfeited amounts to resident payments and mitigation purposes consistent with this article.
(5) Reinstatement. The administrator may adopt rules allowing reinstatement only upon a sustained period of verified compliance, remediation of harms, and payment of any outstanding amounts and penalties. Reinstatement does not waive remedies for the period of noncompliance.

(6) Conditional settlement benefits. Any release, safe harbor, reduced-liability schedule, or other limitation on remedies provided through MSSA participation is expressly conditioned on ongoing compliance. The MSSA participation agreement shall state that material breach may result in termination of settlement benefits and, to the extent permitted by law and the terms of the agreement, revival of claims or remedies otherwise released or limited for the period of noncompliance.
(7) Cure period; exceptions. Except for fraud, knowing circumvention, or intentional tampering with Audit Markers, registry controls, or Trust safeguards, the administrator shall provide a reasonable opportunity to cure before final disqualification. The cure notice shall specify the violation, required remediation steps, and a cure deadline. Failure to cure constitutes an additional basis for disqualification.
(8) Nonrefundable contributions; liquidated damages characterization. Contributions, assessments, or payments made pursuant to MSSA participation are nonrefundable and are deemed earned upon receipt to fund resident payments, mitigation, auditing, and enforcement costs. Where forfeiture applies under subsection (4), the General Assembly finds that the amounts reflect a reasonable estimate of hard-to-measure public mitigation and enforcement costs and are intended as liquidated damages and cost recovery, not as a punitive fine.

> (2) It is the intent of the general assembly that this Act: (a) Define and protect The Digital Soul as inalienable intangible personal property; (b) Establish the Master Deed registry as the official record of resident digital property rights; (c) Create Audit Markers as verifiable statutory-damage triggers for unauthorized use detection; (d) Authorize and direct the Master Data Settlement and Restitution Agreement process; (e) Establish the Data Tap financial routing system connecting to the Enterprise Mitigation Revenue under article 20 of title 24; (f) Build Civic Access Infrastructures including myColorado ID

physical kiosks with Joint Household Veto Power; and (g) Direct the General Assembly to refer a constitutional amendment to the voters.

SECTION 2. In Colorado Revised Statutes, add article 15 to title 15 as follows:

ARTICLE 15 — PERSONAL DATA AND DIGITAL PROPERTY RIGHTS

15-15-101. ***Definitions.***

As used in this article 15, unless the context otherwise requires:

(1) "The personal data and derived inferences" means the totality of a resident's digital identity and emergent automation-generated property, including: (a) biometric data — any data derived from a resident's physical or physiological characteristics, including fingerprints, retinal scans, facial geometry, voiceprints, gait patterns, DNA sequences, and physiological signals; (b) behavioral data — any data derived from a resident's habits, routines, preferences, patterns of movement, purchasing decisions, communication patterns, or other behavioral attributes; (c) derived biological data — any inference, prediction, score, profile, or classification derived from biometric or behavioral data, including health risk scores, emotional state assessments, neurological inferences, and fertility or vulnerability indicators; (d) civic telemetry — location data, transit data, voting and civic participation data, government service interaction records, and infrastructure usage data; and (e) all emergent automation-generated inferences derived from any of the foregoing. The personal data and derived inferences is the inalienable intangible personal property of the resident from whom it derives. No covered entity may assert ownership, perpetual license, or lien against The personal data and derived inferences.

(2) "Master Deed" means the official digital property rights record establishing a resident's ownership of their personal data and derived inferences, registered with the state, cryptographically anchored in the Colorado Trust of Unique and Identifying Information, and accessible by the resident through the myColorado platform or Civic Access Infrastructure.

(3) "Audit Marker Signature" means a uniquely-tagged, synthetically generated data artifact embedded within a resident's personal data and derived inferences profile — invisible in ordinary use — that serves as an irrefutable, cryptographically verifiable evidence marker of unauthorized ingestion, scraping, or training, triggering automatic statutory damages upon detection.

(4) "Resident Automated Mitigation Account" means the resident-controlled account within the Colorado Automation Mitigation Trust established under article 20 of title 24 that receives Premium Royalty payments triggered by Tier 2 Data Tap events under section 15-15-110.

ROYALTY FLOOR. ***Minimum per-person annual royalty; CPI-indexed.***

(1) Minimum annual royalty. Where this article requires or authorizes payment of a royalty, dividend, or compensation amount to a resident for authorized use of the resident’s protected data, inferences, or derived works, the payment schedule shall include a minimum annual royalty floor per eligible resident.
(2) Floor amount. The minimum annual royalty floor is two hundred fifty dollars ($250) per eligible resident per covered operator, per calendar year, unless a higher floor is established by rule. The floor is adjusted annually for inflation under the inflation adjustment section of this article.
(3) Pro-rata and de minimis. The administrator may adopt rules to pro-rate the floor for partial-year eligibility and to prevent duplicative payment where multiple controlled affiliates are treated as a single operator, but shall not set a de minimis threshold that defeats the floor.

(5) "Master Data Settlement and Restitution Agreement" or "Legacy Use Settlement Agreement" means an enforceable agreement entered between the attorney general and a historical violator under section 15-15-130, resolving claims arising from unauthorized Digital Soul extraction, training, scraping, or monetization occurring prior to the effective date of this article.

(6) "Legacy Use Settlement Program" means the Legacy Use Settlement Agreement enforcement strategy authorized under section 15-15-130 by which the attorney general leverages the combined weight of statutory damages triggered by Audit Markers, enterprise assessments under article 20 of title 24, and existing AG enforcement powers to compel historical violators into comprehensive settlements.

(7) "Digital Deed" means the enforceable legal title instrument embedded within a resident's Master Deed that specifies the resident's consent grants, restrictions, royalty entitlements, and Generative Veto rights with respect to specific categories of the resident's personal data and derived inferences.

(8) "Generative Veto" means a resident's right to prohibit any covered entity from using the resident's personal data and derived inferences to generate, train, fine-tune, augment, or produce any synthetic output, model output, or downstream commercial product.

(9) "Mandatory Disconnection" means a resident's right to demand that a covered entity permanently delete, purge, and certifiably destroy all copies of the resident's personal data and derived inferences data, including training corpora, model weights, and embeddings, within the timeframes established by rule.

(10) "Analog " means a designated physical space in which a resident has activated the Non-Networked Isolation Protocol, exercising their right to an analog environment free from automated sensing, capture, or automated-mediated interaction.

(11) "Compute Parity" means a resident's right to access the same quality, capability, and feature tier of covered automation services available to commercial customers of the covered entity, without algorithmic downgrade, throttling, or capability restriction based on the resident's personal data and derived inferences consent profile or exercise of rights under this article.

(12) "Civic Access Infrastructure" means the physical access infrastructure established under section 15-15-140, including myColorado ID kiosks at county centers, that enables residents without digital access to exercise all rights under this article, including Master Deed registration, transactions, consent updates, and loading of Resident Automated Mitigation Account benefits cards or linked bank accounts.

(13) "Joint Household Veto Power" means the consent right established under section 15-15-141 by which a lawfully married spouse or registered domestic partner may co-sign or veto consent grants, royalty disbursements, or Resident Automated Mitigation Account transactions on behalf of the household, subject to individual resident primacy and anti-coercion safeguards.

(14) "Restoration Credits" means non-cash mitigation credits issued by the CCPAME for the limited purpose of defraying measurable externalities arising from Emergent Automation, redeemable only through direct-to-provider payment rails or other fiduciary spend-control protocols. Restoration Credits are not cash and may not be withdrawn as cash.

(15) "Covered entity" means any person or business entity that deploys, operates, offers, sells, licenses, leases, or provides a covered emergent automation system in Colorado, or that commercially delivers such a system to or targets Colorado residents.

(16) "Intake Firewall" means the technical and contractual control system through which a covered entity verifies consent before ingesting, processing, or training on Digital Soul data.

(17) "Decentralized Identity Verification Protocol" means a cryptographically verifiable, resident-issued consent signal anchored to the resident's Master Deed, constituting valid consent for a specific, scoped use of Digital Soul data.

THE DIGITAL SOUL AS INALIENABLE PROPERTY — MASTER DEED

15-15-102. The Digital Soul — Inalienable Intangible Personal Property — No Waiver — No Conversion.

(1) Inalienability. The Digital Soul is the inalienable intangible personal property of the resident from whom it derives. A resident's ownership of their Digital Soul: (a) cannot be waived, assigned, forfeited, or surrendered by any contract, terms-of-service agreement, or consent form, except through the limited, revocable, scoped consent mechanisms established in this article; (b) cannot be levied upon, liened, garnished, or taken in satisfaction of any debt or obligation of the resident except as authorized by court order under procedures established by rule; (c) survives the resident's death and passes to their designated heir or estate as intangible personal property.

(2) No perpetual license. Any contract term, terms-of-service clause, license grant, or data-processing agreement purporting to convey a perpetual, irrevocable, or royalty-free license to a resident's Digital Soul is void ab initio as against public policy.

(3) Consent revocability. Any consent granted by a resident for use of Digital Soul data is revocable at will, subject to reasonable technical wind-down periods established by rule, not to exceed ninety (90) days.

15-15-103. ***Master Deed Registry — Registration — Digital Deed Instrument — Cryptographic Anchoring.***

(1) Establishment. The secretary of state, in coordination with the ODO established under title 10, article 10, shall establish and maintain the Master Deed Registry as the official state record of resident digital property rights.

(2) Registration. Any Colorado resident may register a Master Deed, at no cost, through: (a) the myColorado digital platform; or (b) an Civic Access Terminal at any county service center, subject to section 15-15-140.

(3) Digital Deed instrument. A Master Deed shall include one or more Digital Deed instruments specifying: (a) the categories of Digital Soul data the resident authorizes for use; (b) the specific purposes, time limits, and royalty rates applicable to each authorization; (c) any Generative Veto, Mandatory Disconnection demands, or Analog designations; and (d) the resident's Resident Automated Mitigation Account routing information for Premium Royalty payments.

(4) Cryptographic anchoring. Each registered Master Deed shall be cryptographically anchored as a Resident Identity Verification Hash in the Colorado Trust of Unique and Identifying Information established under title 10, article 10, creating an immutable, verifiable record of the resident's digital property rights.

(5) Interoperability. The secretary of state shall establish a standard API enabling covered entities to query Master Deed consent status for Digital Soul data categories, subject to privacy-preserving, zero-knowledge verification methods that do not expose the resident's full Master Deed to the querying entity.

SYNTHETIC DATA INTEGRITY MARKER SIGNATURES — STATUTORY DAMAGES TRIGGER

15-15-104. Audit Markers — Unauthorized Ingestion Detection — Statutory Damages.

(1) Authority and purpose. The ODO shall develop and maintain a library of Audit Markers — uniquely-tagged synthetic data artifacts — that may be registered by residents within their Master Deed profiles for the purpose of detecting unauthorized ingestion, scraping, or training by covered entities.

(2) Activation and embedding. A resident may, through their Master Deed registration or Civic Access Infrastructure, activate one or more Audit Markers to be embedded within their Digital Soul profile. The resident shall not be required to disclose the specific nature or location of embedded Audit Markers to any covered entity.

(3) Detection and automatic trigger. When the ODO detects that a Audit Marker Signature has appeared in a covered entity's model outputs, training data, or inference pipeline — demonstrating unauthorized ingestion — the detection event shall: (a) constitute conclusive, irrefutable evidence of unauthorized use of the associated resident's Digital Soul without a valid Decentralized Identity Verification Protocol; (b) automatically trigger statutory damages under subsection (4); and (c) constitute a predicate act for the Legacy Use Settlement Agreement Legacy Use Settlement Program under section 15-15-130.

(4) Statutory damages. Upon confirmed Audit Marker detection, the affected resident shall be entitled to statutory damages of not less than: (a) five thousand dollars ($5,000) per detected unauthorized use; (b) ten thousand dollars ($10,000) per detected Audit Marker where the unauthorized use involved generation of a synthetic likeness of the resident; (c) twenty-five thousand dollars ($25,000) per detected Audit Marker where the unauthorized use involved the resident's biometric or derived biological data. Statutory damages accrue per violation and are cumulative. They do not require proof of actual damages.

(5) AG referral and class aggregation. The ODO shall transmit Audit Marker detection events to the attorney general for enforcement. The attorney general may aggregate individual Audit Marker detection events across residents into a class enforcement action or as predicates for an Legacy Use Settlement Agreement proceeding under section 15-15-130.

(6) Covered entity liability. A covered entity that has ingested a Audit Marker Signature is strictly liable for the statutory damages in subsection (4). It is not a defense that the ingestion was automated, inadvertent, or conducted by a contractor or processing partner.

MASTER SETTLEMENT AND SOVEREIGNTY AGREEMENT — ROPE-A-DOPE

15-15-130. Master Settlement and Master Data Settlement and Restitution Agreement — Legacy Use Settlement Agreement — Legacy Use Settlement Program Enforcement Strategy — Historical Violator Compulsion.

(1) Purpose and authority. The attorney general is authorized and directed to pursue Master Settlement and Master Data Settlement and Restitution Agreements with covered entities that have engaged in historical violations — the unauthorized extraction, scraping, ingestion, training upon, or commercial monetization of Colorado resident Digital Soul data prior to or after the effective date of this article. The Legacy Use Settlement Agreement mechanism, known as the Legacy Use Settlement Program, leverages the combined weight of: (a) Audit Marker statutory damages under section 15-15-104; (b) enterprise assessments and Digital Severance Assessments under article 20 of title 24; (c) existing attorney general enforcement powers under the Colorado Consumer Protection Act and the Colorado Privacy Act; and (d) reputational and market-access consequences of non-settlement to compel comprehensive remediation agreements.

(2) Legacy Use Settlement Agreement components. An Legacy Use Settlement Agreement negotiated under this section shall include, at minimum: (a) a full accounting and disclosure of all Colorado resident Digital Soul data ingested, trained upon, or monetized; (b) retroactive royalty payments calculated using the Digital Severance Assessment rates in section 24-20-116, applied to all historical severance events; (c) a forward-going compliance plan, including Intake Firewall deployment, Decentralized Identity Verification Protocol integration, and Master Deed API compliance; (d) a resident restitution fund, administered through the Colorado Automation Mitigation Trust under

article 20 of title 24, for distribution to affected residents whose Audit Markers were detected or who can demonstrate unauthorized use of their Digital Soul; and (e) enhanced monitoring and reporting obligations for a period of not less than five (5) years.

(3) Legacy Use Settlement Program sequencing. The attorney general shall implement the Legacy Use Settlement Agreement Legacy Use Settlement Program in the following sequence: (a) Phase 1: Audit Marker activation — the ODO activates and embeds Audit Markers across the resident population, beginning to accumulate irrefutable evidence of unauthorized use by covered entities; (b) Phase 2: Assessment notices — the CCPAME issues Digital Severance Assessment notices and enterprise fee obligations to historical violators, creating an escalating financial pressure; (c) Phase 3: Legacy Use Settlement Agreement demand — the attorney general transmits Legacy Use Settlement Agreement demand letters to identified historical violators, presenting the aggregated Audit Marker evidence and financial exposure; (d) Phase 4: Negotiation — the attorney general conducts settlement negotiations, with the understanding that failure to settle results in full statutory damages, treble damages for willful conduct, and public enforcement action; (e) Phase 5: Settlement or litigation — the attorney general executes an Legacy Use Settlement Agreement or initiates formal litigation.

(4) No statute of limitations waiver required. The Legacy Use Settlement Agreement mechanism operates prospectively from the effective date of this article. The attorney general's existing legal authority governs any claims regarding conduct prior to the effective date, and this section does not constitute a limitation or waiver of any such authority.

(5) Public Legacy Use Settlement Agreement registry. The attorney general shall maintain a public registry of executed Legacy Use Settlement Agreements, including the identity of the settling entity, the scope of the agreement, the total restitution fund established, and the compliance monitoring obligations, subject to redaction of protected trade secrets and individual resident information.

DATA TAP FINANCIAL ROUTING — TIER 1 AND TIER 2

15-15-110. Data Tap Financial Routing — Tier 1 Base Dividend — Tier 2 Premium Royalty — Resident Automated Mitigation Account.

(1) Purpose. Enterprise Mitigation Revenue mechanism is the financial routing mechanism that connects resident Digital Soul property rights to the Enterprise Mitigation revenue system under article 20 of title 24, ensuring that every commercial use of Digital Soul data generates a resident financial benefit.

(2) Tier 1 — Anonymous data — Base Dividend. When a covered entity uses Digital Soul data that has been verified as anonymized or de-identified, consistent with objective standards established by rule, the Colorado Trust of Unique and Identifying Information shall generate a Tier 1 Data Tap signal. The Tier 1 signal triggers a Base Dividend calculation, with proceeds flowing into the Colorado Automation Mitigation Trust under article 20 of title 24 for distribution as part of the Enterprise Mitigation

Revenue, including child solvency funds, mental health interventions, housing stabilization, and analog bridge infrastructure.

(3) Tier 2 — Identifying data — Premium Royalty. When a covered entity uses Digital Soul data that contains personally identifying information, distinct persona links, or Digital Soul attributes that can identify or re-identify a resident, the Colorado Trust of Unique and Identifying Information shall generate a Tier 2 Data Tap signal. The Tier 2 signal triggers a Premium Royalty calculation. Premium Royalty proceeds shall be routed directly to the individual resident's Resident Automated Mitigation Account via the Colorado Trust. Premium Royalty payments are the resident's private property and may be disbursed as cash, loaded onto a linked benefits card or bank account, or applied to Restoration Credits at the resident's election.

(4) Rate schedule. The CCPAME shall establish, by rule, the Base Dividend and Premium Royalty rate schedule, calibrated to the Digital Severance Assessment rates in section 24-20-116. The rate schedule shall ensure that Tier 2 Premium Royalty rates are materially higher than Tier 1 Base Dividend rates, creating a persistent financial incentive for covered entities to obtain full Decentralized Identity Verification Protocol consent rather than relying on de-identification.

(5) Resident access to Resident Automated Mitigation Account. A resident may access their Resident Automated Mitigation Account through the myColorado platform or any Civic Access Terminal, including for cash disbursement, card loading, bank account transfer, or allocation to child solvency or household mitigation funds.

CIVIC ACCESS INFRASTRUCTURES AND myColorado ID — SPOUSAL VETO POWER

15-15-140. Civic Access Infrastructures — Physical Kiosk Infrastructure — myColorado ID — Universal Access.

(1) Establishment. The state shall establish and maintain a statewide network of Civic Access Infrastructure access points, located at county service centers, public libraries, and other accessible public facilities, ensuring that every resident — regardless of digital access, technical literacy, or disability status — can exercise all rights under this article in person, through a human-staffed process or a myColorado ID kiosk.

(2) Required Civic Access Infrastructure functions. Every Civic Access Infrastructure access point shall enable a resident to: (a) register, update, or revoke a Master Deed and Digital Deed instruments; (b) submit Mandatory Disconnection demands; (c) activate or deactivate Audit Markers; (d) access their Resident Automated Mitigation Account balance, transaction history, and disbursement options; (e) load Resident Automated Mitigation Account funds onto a linked benefits card or linked bank account; (f) file complaints, submit grievances, and access ODO intake services; and (g) request Legacy Use Settlement Agreement-related restitution fund applications.

(3) myColorado ID integration. The myColorado ID platform shall serve as the digital-physical bridge interface, enabling residents to: (a) authenticate through a physical government-issued ID without requiring a smartphone or internet connection; (b) receive a printed receipt of all transactions and registrations for personal records; and (c) access a human navigator who can assist with complex transactions or special circumstances.

(4) Parity requirement. Civic Access Infrastructure services shall be substantively equivalent in scope, timeliness, and quality to digital platform services. No right under this article may be conditioned on digital access. The state shall ensure that processing times for Civic Access Infrastructure transactions do not materially exceed digital transaction processing times.

(5) Funding. The costs of establishing and maintaining Civic Access Infrastructure infrastructure shall be funded from the Analog Access Implementation Fund established under title 10, article 10, consistent with the fee allocation tables in section 10-10-160.

15-15-141. Joint Household Veto Power — Household Co-Consent and Transaction Co-Authorization.

(1) Purpose. The general assembly finds that Digital Soul rights and Resident Automated Mitigation Account assets are household assets with shared family implications. A resident who is lawfully married or in a registered domestic partnership may designate their spouse or partner to exercise limited co-consent and co-authorization rights over Digital Soul transactions, providing an additional layer of household protection without overriding individual resident primacy.

(2) Scope of Joint Household Veto Power. A resident's designated spouse or domestic partner may, upon written designation by the resident: (a) co-sign or veto consent grants for Digital Soul data uses above a transaction threshold established by rule; (b) co-authorize Resident Automated Mitigation Account disbursements above a household disbursement threshold established by rule; and (c) receive joint notification of Audit Marker detection events and Legacy Use Settlement Agreement restitution fund eligibility determinations affecting the household.

(3) Individual resident primacy. The Joint Household Veto Power does not override individual resident control. A resident may at any time revoke the Joint Household Veto designation unilaterally. A resident's individual consent grant or revocation remains valid notwithstanding the absence of spousal co-signature, except within the transaction thresholds established pursuant to subsection (2).

(4) Anti-coercion safeguards. The secretary of state and the ODO shall establish rules to prevent coercive use of the Joint Household Veto Power, including: (a) automatic suspension of Joint Household Veto authority upon the filing of a protection order, domestic violence allegation, or court order addressing coercion; (b) a resident's right to terminate the Joint Household Veto designation through any Civic Access Infrastructure without spousal co-authorization; and (c) training for Civic Access Infrastructure navigators on recognizing coercion indicators.

(5) Civic Access Infrastructure registration. A Joint Household Veto Power designation may be made, modified, or revoked through the myColorado platform

or any Civic Access Terminal, without requiring digital access or attorney assistance.

DIGITAL SOUL RIGHTS — CORE CONSUMER PROTECTIONS

15-15-105. Intake Firewall — Decentralized Identity Verification Protocol — Consent Architecture.

(1) No covered entity may ingest, process, train on, or commercially monetize any category of Colorado resident Digital Soul data without a valid, cryptographically verifiable Decentralized Identity Verification Protocol anchored to the resident's Master Deed.

(2) Any data ingested without a valid Decentralized Identity Verification Protocol is Contraband Data, subject to the enforcement provisions of title 10, article 10, and the statutory damages provisions of section 15-15-104.

(3) Consent scope. A Decentralized Identity Verification Protocol is valid only for the specific data categories, purposes, time periods, and compensation terms specified in the resident's Digital Deed. Any use beyond the scoped consent is an unauthorized use triggering statutory damages.

15-15-106. ***Generative Veto — Mandatory Disconnection — Right to Destruction.***

(1) Generative Veto. A resident may at any time invoke a Generative Veto through their Master Deed, prohibiting any covered entity from using the resident's Digital Soul to generate, train, fine-tune, augment, or produce any synthetic output, model output, or downstream commercial product.

(2) Mandatory Disconnection. A resident may demand Mandatory Disconnection, requiring a covered entity to permanently delete, purge, and certifiably destroy all copies of the resident's Digital Soul data, including training corpora, model weights, and embeddings, within ninety (90) days of the demand, or a shorter period established by rule.

(3) Certification. A covered entity that receives a Mandatory Disconnection demand shall provide a cryptographically verifiable certification of destruction, filed with the ODO, within the applicable destruction period.

15-15-107. Post-Mortem Data Disposition Directive — Authorized Successor Data Designation — Pre-Digital Property Archive.

(1) Post-Mortem Data Disposition Directive. A resident may include in their Master Deed a Post-Mortem Data Disposition Directive requiring all covered entities holding the resident's Digital Soul data to execute Mandatory Disconnection within ninety (90) days of confirmed notification of the resident's death.

(2) Authorized Successor Data Designation. A resident may designate a Authorized Successor Data Designation — a protected archive of specified Digital

Soul data categories — to be preserved, transferred to a designated heir, or maintained in mitigation custodial custody by the Colorado Trust of Unique and Identifying Information following the resident's death.

(3) Pre-Digital Property Archive. Where a resident does not execute a Post-Mortem Data Disposition Directive or Authorized Successor Data Designation designation, covered entities holding the resident's Digital Soul data shall apply default privacy protections established by rule, preventing commercial use without authorization from the designated heir or estate.

15-15-108. ***NCII Prohibition — Nonconsensual Intimate Imagery — Emergency Injunctive Relief.***

(1) Prohibition. No covered entity may generate, distribute, host, transmit, or commercially benefit from nonconsensual intimate imagery (NCII) involving a Colorado resident, including automated-generated or synthetic NCII.

(2) Strict liability. NCII violations are strict-liability offenses. The existence of NCII attributable to a resident in a covered entity's systems or outputs, without verifiable consent, constitutes the violation.

(3) Emergency injunctive relief. A resident who is a victim of NCII may seek emergency injunctive relief in any court of competent jurisdiction, including an ex parte temporary restraining order requiring immediate takedown, without bond, upon a credible showing of the violation.

(4) Damages. In addition to injunctive relief, a resident who prevails on an NCII claim shall be entitled to: (a) actual damages; (b) statutory damages of not less than twenty-five thousand dollars ($25,000) per violation; and (c) attorney's fees and costs.

15-15-109. ***Minor Protections — Guardianship Credentialing — Dual-Consent Protections.***

(1) No covered entity may ingest, process, or use the Digital Soul data of a minor without the verified, informed consent of the minor's parent or lawful guardian, in addition to the minor's affirmative assent where age-appropriate.

(2) Legacy tracking technologies default-off. All tracking, profiling, and data-retention features for minor residents shall default to off and may be activated only through dual consent — the guardian and the minor (age 13 and over) — with clear, plain-language notice.

(3) Guardian credentialing. A parent or guardian exercising consent rights over a minor's Digital Soul must credential through the Master Deed registry, establishing a guardianship link that is auditable by the ODO and terminates automatically upon the minor reaching majority.

CONSTITUTIONAL AMENDMENT DIRECTIVE

15-15-150. Constitutional Amendment Directive — General Assembly Referral — Digital Soul as Inalienable Property Under the Colorado Constitution.

(1) Findings. The general assembly finds that the rights established in this article — the ownership of The Digital Soul as inalienable intangible personal property — are so fundamental to resident sovereignty, economic participation, and protection from emergent automation harms that they require constitutional protection against future legislative erosion.

(2) Directive to the General Assembly. The general assembly is hereby directed, not later than the first general session following the effective date of this act, to: (a) draft a proposed constitutional amendment to the Colorado Constitution that enshrines The Digital Soul — including biometric data, behavioral data, derived biological data, and civic telemetry — as inalienable intangible personal property of every Colorado resident; (b) include in the proposed amendment the protections of the Master Deed, the Generative Veto, and the right to Mandatory Disconnection as fundamental resident rights that no future legislative act may abrogate without voter approval; and (c) refer the proposed constitutional amendment to the voters of Colorado at the next general election occurring at least ninety (90) days after the date of referral.

(3) Proposed amendment scope. The proposed constitutional amendment shall, at minimum: (a) define The Digital Soul as the biometric, behavioral, derived biological, and civic telemetry data of a resident, along with all emergent automation-generated inferences derived therefrom; (b) declare The Digital Soul to be the inalienable intangible personal property of the resident, co-equal in dignity and legal protection with tangible personal property; (c) prohibit any law, contract, terms-of-service agreement, or government act that purports to permanently alienate, waive, or extinguish a resident's Digital Soul rights without just compensation and voter approval; and (d) guarantee the Symbiotic Sovereignty principle — that a resident's digital existence and physical existence are inseparable, and that the rights of one cannot be severed from the other without the resident's free, informed, and revocable consent.

(4) Savings; statutory rights preserved pending amendment. The rights established in this article are enforceable as statutory rights pending voter approval of any constitutional amendment and shall not be diminished or suspended pending the referendum.

(5) Ballot language. The general assembly shall cause the proposed constitutional amendment to be placed on the ballot with language approved by the title board that clearly and accurately describes to voters: (a) the meaning of The Digital Soul as personal property; (b) the nature of the Symbiotic Sovereignty principle; and (c) the specific rights and protections to be constitutionalized.

OPTION B — PHASED SCALE-UP — CAPABILITY PARITY

15-15-114. ***Phased Compliance — Option B Scale-Up — Privacy Minimization — Payment Rail Privacy.***

(1) General. Covered entities shall come into compliance with this article according to the phased schedule and option pathways established by rule, provided that all entities shall be in full compliance not later than three (3) years after the effective date of this act.

(2) Option B — phased scale-up with privacy minimization. A covered entity that elects Option B compliance shall implement the Intake Firewall and Decentralized Identity Verification Protocol architecture on a phased schedule established by rule, provided that: (a) the entity demonstrates a good-faith compliance roadmap within ninety (90) days of the effective date; (b) privacy minimization is implemented in each phase, reducing unauthorized ingestion progressively; and (c) full compliance is achieved within the deadline established in subsection (1).

(3) Payment rail privacy by design. Any payment processing or compensation infrastructure used to route Premium Royalty or Base Dividend payments to residents shall be designed with privacy-by-default, ensuring that payment transactions cannot be used to profile, track, or re-identify residents.

(4) Capability parity. No covered entity shall algorithmically downgrade, throttle, or deny Compute Parity to a resident based on the resident's exercise of Digital Soul rights, consent profile, or Generative Veto. Violation of this section constitutes a deceptive trade practice under the Colorado Consumer Protection Act.

INFLATION ADJUSTMENT. ***Inflation adjustment for fixed-dollar amounts.***
(1) Any fixed-dollar amount, threshold, cap, minimum, maximum, penalty, statutory damages amount, or fixed-dollar rate set forth in this article shall be adjusted annually on January 1 by the administrator to reflect inflation. The adjustment must be based on the Consumer Price Index for All Urban Consumers (CPI-U), U.S. City Average, as published by the Bureau of Labor Statistics, or a successor index. The base year is the first full calendar year in which this article is operative.
(2) The administrator shall publish the adjusted amounts no later than December 1 of each year for the following calendar year, rounded to the nearest whole dollar. This section does not apply to amounts expressed as a percentage, a market-indexed benchmark, or a formula that automatically adjusts with price level.

SECTION 3. SEVERABILITY

If any provision of this act or its application is found invalid, such invalidity does not affect other provisions that can be given effect without the invalid provision. The provisions of this act are declared severable.

SECTION 4. SAFETY CLAUSE

The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

AMPLIFY Act — Bill 1: Personal Data and Digital Property Rights Act

additions: Digital Soul property definition | Legacy Use Settlement Agreement Legacy Use Settlement Program | Audit Markers | Data Tap Tier 1/2 | Civic Access Infrastructure | Joint Household Veto Power | Constitutional Amendment Directive

CONSTRUCTION; SCOPE OF COMMERCIAL PROCESSING.

(1) For purposes of this act, “commercial processing” includes collection, scraping, ingestion, training, fine-tuning, evaluation, storage, labeling, or other use of resident Digital Soul data when conducted by or for a covered operator in connection with a product, service, system, or capability that is offered, licensed, used, or deployed in commerce, whether or not the specific processing step is described as research, development, testing, or internal evaluation.

(2) A covered operator shall not evade the consent and Master Deed authorization requirements by characterizing a monetizable data ingestion or training pipeline as noncommercial research.

IMPLEMENTATION SCHEDULE — TIERED PHASE DEPLOYMENT

15-15-900. Implementation schedule.

(1) Immediate rights and protections.
The following provisions take effect immediately upon enactment of this act:

(a) Recognition of the Digital Soul as resident-owned intangible personal property.
(b) Enforceability of Master Deed authorization and consent controls.
(c) Prohibition on unauthorized extraction or commercial processing of the Digital Soul.
(d) Establishment of the Colorado Trust of Unique and Identifying Information.
(e) Authorization of the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME).
(f) Authorization of the Colorado Automation Mitigation Trust.
(g) Authority for responsible agencies to promulgate rules necessary to implement this act.

These provisions constitute self-executing statutory rights and are not dependent upon technical system deployment.

(2) Phase I — Administrative establishment (0–12 months).
Responsible agencies shall establish:

(a) the Colorado Trust of Unique and Identifying Information;
(b) the Colorado Automation Mitigation Trust;
(c) enterprise accounting mechanisms for the Enterprise Mitigation Revenue;
(d) rulemaking for Master Deed authorization standards, inter-system monitoring standards, and enterprise compliance reporting.

(3) Phase II — Compliance infrastructure (12–24 months).
Covered operators shall implement:

(a) tamper-evident metering systems;
(b) inter-system safety monitoring controls;
(c) incident detection telemetry;
(d) Digital Soul consent verification mechanisms.

During this phase the following revenue mechanisms activate:
High-Density Compute Grid Surcharge, Autonomous Kinetic Asset Registration, Silicon-to-Carbon Reclamation Assessment, and the Algorithmic Risk Pool.

(4) Phase III — Public mitigation programs (24–36 months).
The state shall deploy:

(a) staggered civic infrastructure loans at 1%, 2%, and 3% APR;
(b) mitigation programs funding child solvency, housing stabilization, and healthcare or mental-health services.

Interest collected through civic infrastructure loans shall be swept into mitigation accounts within the Colorado Automation Mitigation Trust.

(5) Phase IV — Long-term stability and oversight (36 months onward).

The following provisions become fully operational:

(a) the Statutory Revenue Floor and dynamic rate adjustments;
(b) workforce displacement transition and vocational reskilling programs;
(c) full enterprise audit cycles and public reporting requirements.

15-15-140. Data Tap; tiered routing; Base Dividend; Premium Royalty.

(1) Tier 1 — anonymous routing. Tier 1 extraction of the Digital Soul that is processed only in anonymous or aggregated form shall remit a Base Dividend to the Colorado Automation Mitigation Trust pursuant to title 24, article 20.

(2) Tier 2 — identifying routing. Tier 2 extraction of the Digital Soul that includes identifying processing shall remit a Premium Royalty routed to the resident's Resident Automated Mitigation Account through the Colorado Trust of Unique and Identifying Information, subject to Master Deed authorization.

(3) Mathematical routing requirement. Covered operators shall implement accounting controls that separately meter Tier 1 and Tier 2 processing volumes and shall remit payments under this section according to rules adopted pursuant to title 24, article 20. Tier 2 processing is prohibited absent Master Deed authorization.

15-15-160. Heritage assets; analog-era vehicles; mechanical sanctuary.

(1) Definitions. For purposes of this section:

(a) “Heritage asset” means an analog-era vehicle that is maintained for personal use and that satisfies the physical barrier requirements of subsection (2) of this section.

(b) “Physical barrier” means a verifiable mechanical override that physically disconnects all external telemetry pathways and disables externally addressable automated kinetic control interfaces, such that remote connectivity cannot be restored without physical intervention.

(2) Certification. The administering agency shall establish a certification process to verify that a vehicle meets the physical barrier requirements necessary to qualify as a pre-digital mechanical asset.

(3) Privacy shield; prohibited mandates. For a certified pre-digital mechanical asset, a state agency, political subdivision, or state contractor shall not require:

(a) continuous connectivity;

(b) installation of externally addressable telemetry modules; or

(c) over-the-air updates as a condition of registration, inspection, insurance eligibility, or operation within the state.

(4) Construction. This section does not limit lawful safety recalls that can be accomplished without removing or defeating a certified physical barrier.

15-15-170. Joint Household veto power for shared family interfaces.

(1) Applicability. If a covered operator offers a shared family interface that permits access to, control of, or authorization over Digital Soul processing for more than one resident within a household, the covered operator shall provide a mechanism for spousal veto as described in this section.

(2) Veto authority. A spouse or civil union partner with shared-interface authority may revoke or withhold authorization for Tier 2 identifying Data Tap routing and for any shared-interface permissions that enable identifying processing of that spouse's Digital Soul, notwithstanding conflicting interface settings initiated by another household user.

(3) Verification and logging. The covered operator shall verify the identity of the vetoing party using Master Deed authorization controls and shall record the veto event in an immutable authorization log.

(4) Construction. Nothing in this section authorizes a spouse to consent to identifying processing of another resident's Digital Soul without that resident's Master Deed authorization.

INDEPENDENT OPERABILITY; COORDINATION; SEVERABILITY.

(1) Independent operability. This act is intended to be independently operable and enforceable. No duty, authority, remedy, assessment, program, or right created by this act is conditioned on the enactment, adoption, or effectiveness of any other measure.

(2) Coordination. If another measure concerning the Digital Soul, the Colorado Automation Mitigation Trust or Enterprise Mitigation Revenue, the Colorado Trust of Unique and Identifying Information, or any related public utility or enterprise framework is enacted, the responsible agencies may coordinate implementation to avoid duplication; however, coordination is permissive and does not limit or delay enforcement of this act.

(3) Harmonization of definitions. If another enacted measure defines terms also used in this act, the definitions shall be construed harmoniously to the greatest extent possible. If an irreconcilable conflict exists, the definition in this act controls for purposes of this act.

(4) Severability. If any provision of this act or its application is held invalid, the invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application.

(5) Rights are immediate. The recognition of the Digital Soul as inalienable intangible personal property and the Master Deed authorization requirements are self-executing and apply immediately upon enactment, regardless of whether any enterprise, trust, or utility program is established by any other measure.

ANNEX — DEFINITIONS ALIGNMENT AND CONTROLLING TERMS

The following definitions govern any conflict between this act and companion documents. The definition in this act controls in all cases.

Controlling term: 'The Digital Soul' (§15-15-101(1)) is the operative statutory term throughout. References in companion documents to 'resident digital identity information' or 'personal data' shall be construed to mean The Digital Soul as defined herein.

Controlling term: 'Master Data Settlement and Restitution Agreement' (Legacy Use Settlement Agreement) supersedes any prior reference to 'Master Settlement and Master Data Settlement and Restitution Agreement' in all companion documents.

Controlling term: 'Pre-Digital Operations Zone' supersedes the truncated 'Analog' reference in §15-15-101(10) of prior drafts.

Controlling term: 'Colorado Automation Mitigation Trust' (§24-20-104, title 24, article 20) supersedes any prior designation for this trust' in all companion documents.

Controlling term: 'UFIPA Income Distribution' (§24-20-157) means the annual distribution of Net Income Receipts from Colorado Automation Mitigation Trust investment holdings to registered Master Deed holders, independent of and additive to the Resident Mitigation Dividend. Residents receive both distributions annually from their Resident Automated Mitigation Account.

Controlling term: 'Statutory Rate Schedule' (§24-20-156) means the binding rate schedule with floors, initial rates, and ceilings for all Enterprise Mitigation fees. CCPAME may only move rates within the statutory band. Harmonization rule: In the event of any irreconcilable conflict between a definition in this act and a definition in any companion document, fiscal impact statement, or administrative record, the definition in this act controls for purposes of this act.

FEDERAL PREEMPTION SAVINGS CLAUSE

Federal preemption. This act shall operate to the maximum extent permitted by federal law. If any provision of this act is found to be preempted by federal law, that provision is severable pursuant to the severability clause of this act, and the remaining provisions continue in full force and effect. Nothing in this act shall be construed to conflict with the Supremacy Clause of the United States Constitution; rather, this act is expressly designed to operate within Colorado's reserved powers under the Tenth Amendment to regulate intrastate commercial activity, protect Colorado residents' property rights, and impose fees for measurable externalities caused by covered automation activity within Colorado. To the extent any provision may be construed to conflict with federal law, the CCPAME shall interpret and administer this act in a manner that avoids such conflict while preserving the maximum scope of resident protection authorized under state law.

APPROPRIATION NOTE

No General Fund appropriation required. This act does not require an appropriation from the Colorado General Fund. The Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME) is a government-owned business enterprise funded entirely by enterprise mitigation revenues collected from covered operators under this act. Startup administrative costs incurred prior to initial enterprise mitigation revenue collections are authorized as a contingency loan from the General Fund, to be repaid from first-year enterprise mitigation revenues within eighteen (18) months of the CCPAME's first revenue collection event. This loan authorization does not constitute a continuing appropriation.

AMPLIFY ACT v28 — SUPPLEMENTAL SECTIONS

Minor Digital Soul Trust · Intestate Digital Soul Inheritance · Mandatory Investment Reserve Floor

§15-15-162 (Bill 1) · §15-15-163 (Bill 1) · §24-20-154 Amendment (Bill 3)

SECTION 15-15-162. MINOR DIGITAL SOUL TRUST — GUARDIAN AD LITEM REGISTRATION — LOCKED ACCOUNT — STATE AGENCY PROHIBITION — MAJORITY TRANSFER

15-15-162. Minor Digital Soul Trust — establishment — Guardian Ad Litem Master Deed registration for children in state custody — locked Resident Automated Mitigation Account — categorical prohibition on state agency access — compounding accumulation — full transfer at majority — aging-out payment Dashboard display — Title IV-E administrative funding.

(1) Legislative findings. The general assembly finds and declares that:

(a) Every Colorado resident minor, including every minor in the custody of the Colorado Department of Human Services or any county department of social services, possesses a Digital Soul as inalienable intangible personal property under this article — this property right is not diminished, suspended, or held in abeyance by virtue of the minor's custody status;

(b) Children in foster care, kinship placement, residential treatment, or other state-supervised custody arrangements are among the most vulnerable members of Colorado's digital ecosystem — their behavioral, biometric, health, and communications data is actively processed by covered operators serving or contracted with the child welfare system, generating Enterprise Mitigation Revenue from which the child is entitled to receive royalties and distributions;

(c) The state's historical practice of treating children's accumulated assets as available for cost-of-care recovery, administrative fee offset, or benefits eligibility calculation constitutes a form of institutional asset stripping incompatible with the property rights established in this article;

(d) Federal Title IV-E funding under 42 U.S.C. §670 et seq. provides administrative cost reimbursement to state and county child welfare agencies for eligible children in state custody — the administrative cost of registering a Master Deed on behalf of a child in state custody is a reimbursable administrative activity under Title IV-E, and no child's Resident Automated Mitigation Account funds shall be used to cover any administrative cost of the child welfare system;

(e) A child who ages out of the foster care system in Colorado shall receive every dollar of Digital Soul royalties, UFIPA Income Distributions, and Resident Mitigation Dividend accumulations that accrued during their time in care — compounded, intact, and unencumbered — as a foundation for economic self-sufficiency upon entering adulthood; and

(f) The Minor Digital Soul Trust established by this section is the statutory expression of the general assembly's determination that the child welfare system shall protect children's digital property rights, not profit from them.

(2) Guardian Ad Litem Master Deed registration — mandatory. For every minor in the custody of the Colorado Department of Human Services or any county department of social services:

(a) The court exercising jurisdiction over the minor's custody proceeding shall appoint a Guardian Ad Litem for purposes of Digital Soul property rights registration within thirty (30) days of the custody order, if no parent or legal guardian with authority to register a Master Deed is available and willing to do so. The Guardian Ad Litem appointment for this purpose may be combined with any existing Guardian Ad Litem appointment in the custody proceeding at no additional cost.

(b) The Guardian Ad Litem shall register a Master Deed on behalf of the minor within sixty (60) days of appointment, through the myColorado platform or any Civic Access Terminal, at no cost to the minor or the Guardian Ad Litem.

(c) The Guardian Ad Litem's registration authority is limited to the single act of Master Deed registration and annual renewal. The Guardian Ad Litem has no authority over the minor's Resident Automated Mitigation Account, no withdrawal authority, no investment direction authority, and no authority to consent on the minor's behalf to any covered operator's use of the minor's Digital Soul beyond the minimum necessary for court-ordered services.

(d) No state agency, county department, foster parent, kinship caregiver, or residential placement facility may register a Master Deed on behalf of a minor in state custody. Registration authority is vested exclusively in the Guardian Ad Litem, a parent with legal custody, or the minor themselves upon reaching the age of fourteen (14).

(e) The CCPAME shall maintain a Minor Master Deed Registry — a confidential subregistry of the Master Deed Registry — identifying all minors registered under this subsection and the corresponding locked account status. The Minor Master Deed Registry is not a public record and shall not be disclosed to any state agency except upon court order.

(3) Locked Minor Digital Soul Trust account — structure and protections. Upon Master Deed registration for a minor under subsection (2):

(a) The minor's Resident Automated Mitigation Account is automatically designated as a Locked Minor Digital Soul Trust Account. All Base Dividends, Premium Royalties, UFIPA Income Distributions, Resident Mitigation Dividend payments, and any other distributions accruing to the minor under this article and title 24, article 20 are deposited into the Locked Minor Digital Soul Trust Account and held in trust for the minor's sole benefit until the minor reaches the age of majority or, if the minor is a participant in extended foster care under C.R.S. §26-5.4-101, until the minor reaches the age of twenty-one (21).

(b) All funds in the Locked Minor Digital Soul Trust Account shall be held in interest-bearing instruments consistent with §24-20-157(3), generating compounding returns for the minor's benefit throughout the duration of the trust. The CCPAME shall apply the same investment standards to Locked Minor Digital Soul Trust Accounts as to the Colorado Automation Mitigation Trust Investment Reserve.

(c) The MSMF Child Fund restricted carve-out under §24-20-103(2) applies to Locked Minor Digital Soul Trust Accounts — up to twenty-five percent (25%) of each annual distribution may be released for Child Essentials and birthday and holiday gifts through restricted payment cards as specified in §24-20-103(2). All releases require Guardian Ad Litem authorization and court notification. No release may be made to any state agency or placement facility.

(d) The minor's Locked Minor Digital Soul Trust Account shall be displayed on a confidential minor account dashboard, accessible only to the Guardian Ad Litem and the minor (upon reaching age fourteen), showing current balance, annual accruals, projected majority transfer amount, and historical distribution record.

(4) Categorical prohibitions — state agency access and cost recovery. The following are categorically and unconditionally prohibited:

(a) Any state agency, county department of social services, child welfare contractor, foster care provider, kinship caregiver, or residential placement facility from accessing, withdrawing, garnishing, placing a lien on, or in any way encumbering any funds in a Locked Minor Digital Soul Trust Account;

(b) Any state agency from treating a minor's Locked Minor Digital Soul Trust Account balance or projected distributions as income, assets, or resources for purposes of: (I) foster care cost-of-care recovery or reimbursement calculations; (II) Medicaid or CHP+ eligibility determinations; (III) food assistance, housing assistance, or any other means-tested benefit eligibility calculation; (IV) any administrative fee, placement fee, or service cost assessment;

(c) Any covered operator providing services to the child welfare system — including behavioral health platforms, educational technology providers, case management software vendors, and residential facility management systems — from using a minor's Digital Soul data streams for purposes other than the direct delivery of court-ordered services to that minor, or from assigning a lower Decentralized Identity Verification Protocol consent status to a minor based on their custody status;

(d) Any court from ordering disbursement from a Locked Minor Digital Soul Trust Account for child support, placement costs, legal fees, or any other purpose except direct child welfare expenditures that would otherwise be funded from the minor's own non-Digital Soul assets, and only then with Guardian Ad Litem consent and CCPAME notification; and

(e) Any assignment, voluntary or involuntary, of a minor's rights under this section. The minor's Digital Soul property right and Locked Minor Digital Soul Trust Account rights are non-assignable until the minor reaches majority.

(5) Majority transfer — full and unconditional. Upon the minor reaching the age of majority (or age twenty-one for extended foster care participants under C.R.S. §26-5.4-101):

(a) The entire balance of the Locked Minor Digital Soul Trust Account — including all accumulated principal, UFIPA Income Distributions, Resident Mitigation Dividend payments, MSMF carve-out residuals, and compounded investment returns — transfers unconditionally and automatically to the young adult as their sole and separate property, free and clear of any claim by any state agency, county department, or any person.

(b) The CCPAME shall notify the young adult of the transfer at least ninety (90) days before the transfer date, by physical mail to the last known address and through the myColorado platform, providing the projected transfer amount and instructions for account access.

(c) If the young adult cannot be located within one hundred eighty (180) days of the transfer date, the funds shall be held in the Locked Minor Digital Soul Trust Account for an additional five (5) years with continued compounding before transferring to the Colorado Unclaimed Property Fund — they shall never escheat to the General Fund and shall never be available for child welfare cost recovery.

(d) The CCPAME shall provide every young adult receiving a majority transfer with a written summary of their Digital Soul rights, Master Deed registration status, instructions for accessing the Universal Telemetry Allowance, and information on Resident Data Cooperative membership. This summary shall be available in plain language, in all languages required under §24-20-155 accessibility standards.

(6) Aging-out payment — Public Accountability Dashboard display. The Public Accountability Dashboard required under §24-20-155 shall display, as a separate and prominently featured indicator:

(a) The total number of minors currently registered in the Minor Master Deed Registry (without identifying information);

(b) The aggregate balance of all Locked Minor Digital Soul Trust Accounts statewide (updated quarterly);

(c) The number of majority transfers completed in the current and prior fiscal year;

(d) The average majority transfer amount per young adult in the current and prior fiscal year; and

(e) A running total of all funds transferred to young adults aging out of foster care since the system's inception — labeled: 'Total transferred to young adults aging out of foster care.'

(7) Title IV-E administrative cost funding. The Colorado Department of Human Services shall seek federal reimbursement under Title IV-E of the Social Security Act, 42 U.S.C. §670 et seq., for all administrative costs associated with Guardian Ad Litem Master Deed registration, Minor Master Deed Registry maintenance, and Locked Minor Digital Soul Trust Account administration for Title IV-E eligible children. No administrative cost of the Minor Digital Soul Trust program shall be charged to or offset against any child's Locked Minor Digital Soul Trust Account. If federal reimbursement is unavailable for any cost category, that cost shall be funded from the CCPAME operating budget as a Tier 1 enterprise operating cost under §24-20-151(1).

(8) Enforcement. A violation of any prohibition in subsection (4) is:

(a) A Critical Severity Violation under the enforcement matrix in Annex E, subject to immediate custodial containment of the violating operator's system;

(b) Subject to statutory damages of ten thousand dollars ($10,000) per violation per day, payable directly to the affected minor's Locked Minor Digital Soul Trust Account;

(c) Grounds for immediate disqualification from participation in any state child welfare contract, placement agreement, or service provider arrangement; and

(d) Reportable to the Colorado Attorney General for civil rights enforcement under C.R.S. §24-34-301 et seq.

SECTION 15-15-163. INTESTATE DIGITAL SOUL INHERITANCE — RESIDENT AUTOMATED MITIGATION ACCOUNT SUCCESSION — ANTI-SWEEP PROTECTION — CHILD SOLVENCY FUND RESIDUAL

15-15-163. Intestate succession of Resident Automated Mitigation Account — hierarchy of heirs — prohibition on General Fund escheat — Child Solvency Fund residual — unclaimed property integration — covered operator notification obligation.

(1) Legislative finding. The general assembly finds that the existing Colorado Unclaimed Property Act, C.R.S. §38-13-101 et seq., would, absent express provision in this article, route unclaimed Resident Automated Mitigation Account balances to the General Fund through the standard escheat process — directly circumventing the General Fund sweep prohibition of §24-20-157(9) and the constitutional prohibition in Article XXIX-A §5. This section establishes an express intestate succession rule that routes unclaimed balances to heirs first, the Child Solvency Fund second, and the General Fund never.

(2) Post-Mortem Data Disposition Directive — primary instrument. A registered Master Deed holder's Post-Mortem Data Disposition Directive under §15-15-107 is the primary succession instrument for the Resident Automated Mitigation Account. Where a valid Directive designates a successor, the account transfers to the designated successor within ninety (90) days of the CCPAME's receipt of a certified death certificate, free of any estate claim or probate requirement, as a non-probate transfer on death.

(3) Intestate succession hierarchy — no Directive on file. Where a registered Master Deed holder dies without a valid Post-Mortem Data Disposition Directive, the Resident Automated Mitigation Account balance passes according to the following hierarchy, in order:

(a) Surviving spouse or civil union partner under Colorado intestacy law, C.R.S. §15-11-102;

(b) Surviving children in equal shares, including any minor children whose Locked Minor Digital Soul Trust Accounts receive their share directly;

(c) Surviving parents in equal shares;

(d) Surviving siblings in equal shares;

(e) Any other heir under Colorado intestacy law, C.R.S. §15-11-101 et seq., in the order established by that statute; and

(f) If no heir under subsections (a) through (e) can be identified or located within three (3) years of the Master Deed holder's death, the account balance transfers to the Child Solvency Fund established under §24-20-108 — not to the General Fund, not to the Colorado Unclaimed Property Fund.

(4) Express General Fund escheat prohibition. Notwithstanding the Colorado Unclaimed Property Act, C.R.S. §38-13-101 et seq., or any other provision of Colorado law, no Resident Automated Mitigation Account balance, UFIPA Income Distribution, Resident Mitigation Dividend payment, or any other distribution accruing under this article or title 24, article 20 shall ever escheat to or be transferred to the Colorado General Fund. This prohibition is self-executing. Any transfer in violation of this subsection is void ab initio and shall be reversed by the State Treasurer within ten (10) business days, with interest at the Colorado statutory judgment rate.

(5) Covered operator notification obligation. Upon the death of a registered Master Deed holder, every covered operator holding or processing that resident's Digital Soul data streams shall: (a) immediately cease all commercial use of that resident's Digital Soul data beyond minimum system maintenance requirements; (b) notify the CCPAME of the cessation within thirty (30) days of receiving notice of the resident's death; and (c) make the resident's Digital Soul data streams available for retrieval by the designated successor or intestate heir within sixty (60) days of a valid succession claim. Failure to comply is a Tier 2 Digital Severance violation per record per day of noncompliance.

SECTION 24-20-154 AMENDMENT — MANDATORY INVESTMENT RESERVE FLOOR — PERMANENT FUND INTEGRITY PROTECTION

24-20-154(2)(a) — AMENDMENT. Mandatory minimum Investment Reserve capitalization — ten percent of annual Overflow Pool — prior to Resident Mitigation Dividend calculation — permanent fund integrity — UFIPA income stream long-term protection.

(1) Amendment to §24-20-154(2). Section 24-20-154(2) is amended to add the following mandatory floor provision before the existing discretionary capitalization language:

MANDATORY FLOOR — NEW §24-20-154(2)(a):

(2)(a) Mandatory minimum capitalization — permanent fund integrity. Before the Resident Mitigation Dividend Overflow Pool distribution is calculated under §24-20-153(3) for any fiscal year, the CCPAME shall transfer not less than ten percent (10%) of the total annual Overflow Pool balance into the Colorado Automation Mitigation Trust Investment Reserve as mandatory principal capitalization. This transfer is:

(I) Mandatory — not subject to board discretion, annual appropriation, or any condition other than the existence of an Overflow Pool balance above zero;

(II) Prior in time to the Resident Mitigation Dividend calculation — the 10% floor is removed from the Overflow Pool before per-resident dividend amounts are calculated, so the dividend is calculated on 90% of the Overflow Pool, not 100%;

(III) Additive to the existing discretionary 4/5 board vote capitalization authority — the board retains authority to capitalize the Investment Reserve above the 10% floor as provided in the existing §24-20-154(2); and

(IV) Protected by the Anti-Dilution Ratchet under §24-20-117 — the 10% mandatory floor may only be increased, never decreased, without voter approval.

(2)(b) Rationale — long-term UFIPA income stream protection. The mandatory 10% floor ensures the Investment Reserve grows in proportion to enterprise revenue regardless of current-year dividend pressure. As the Investment Reserve grows, UFIPA Net Income Receipts under §24-20-157 grow proportionally — which increases the UFIPA Income Distribution to residents independently of and in addition to the Resident Mitigation Dividend. The mandatory floor is therefore in residents' long-term interest even though it modestly reduces the current-year dividend: a compounding Investment Reserve eventually produces more resident income than a maximized current-year dividend drawn from a stagnant Reserve.

(2)(c) Public Accountability Dashboard display. The Public Accountability Dashboard under §24-20-155 shall display: (I) the mandatory 10% Investment Reserve transfer amount for the current year; (II) the resulting Overflow Pool balance available for Resident Mitigation Dividend calculation after the mandatory transfer; (III) the current Investment Reserve balance and cumulative mandatory transfers since inception; and (IV) the projected additional per-resident UFIPA Income Distribution attributable to current-year mandatory Investment Reserve growth, updated annually.

SUMMARY — THREE NEW PROVISIONS AND THEIR EFFECTS

Section	What It Does	Who Benefits	Political Effect
§15-15-162 Minor Digital Soul Trust	Guardian Ad Litem registers Master Deed for every child in state custody. Account locked until majority — fully compounding. State agency access categorically prohibited. Full balance transfers at age 18/21 to young adult, unencumbered. Violations are Critical Severity with $10K/day damages to the child's account.	Every child in Colorado foster care, kinship placement, or residential treatment — approximately 12,000-15,000 children annually	Politically unassailable. Creates powerful aging-out constituency. Pre-Digital Mechanical Asset owners + foster care advocates + child welfare reform community = broad coalition. Dashboard line showing 'Total transferred to young adults' becomes most-watched number in the system.
§15-15-163 Intestate Digital Soul Inheritance	Explicit intestate hierarchy routes unclaimed accounts to heirs first, Child Solvency Fund second, General Fund never. Express override of Unclaimed Property Act escheat. Covered operators must cease commercial use of deceased resident's Digital Soul and make data available to heirs.	All registered Master Deed holders and their families. Child Solvency Fund benefits from residual rather than General Fund	Closes the sweep prohibition back door. Prevents unclaimed property law from being used as an end-run around §24-20-157(9). Family property rights narrative reinforces the constitutional amendment campaign.
§24-20-154(2)(a) Mandatory	10% of annual Overflow Pool transferred to Investment Reserve before dividend calculation — mandatory, not discretionary. Anti-	All current and future Master Deed holders — current-year dividend slightly lower; long-term	Protects the permanent fund character of the system against future political pressure to maximize short-term dividends.

Investment Reserve Floor	Dilution Ratchet protected. Increases UFIPA income stream long-term while modestly reducing current-year dividend.	UFIPA distributions significantly higher as Reserve compounds	Makes the Phase 2 constitutional argument stronger: 'We built a permanent fund, not a slush fund.'

AMPLIFY Act v28 — §§15-15-162, 15-15-163, §24-20-154(2)(a) Amendment
Minor Digital Soul Trust · Guardian Ad Litem Registration · Categorical Agency Prohibition · Full Majority Transfer · Intestate Succession Anti-Sweep · Mandatory 10% Investment Reserve Floor

AMPLIFY ACT v28 — RESIDENTIAL AI GATEWAY

§10-10-305 (Bill 2) · §15-15-165 (Bill 1)

Residential AI Gateway Device — Civic Utility Perimeter Infrastructure — Edge-Computed Compliance — Home Sanctuary Physical Override — Joint Household Consent — 30-Day Symmetrical Notice Standard

SECTION 10-10-305. RESIDENTIAL AI GATEWAY DEVICE — CIVIC UTILITY PERIMETER INFRASTRUCTURE — EDGE-COMPUTED COMPLIANCE — FOURTH AMENDMENT ARCHITECTURAL STANDARD — 30-DAY SYMMETRICAL NOTICE

10-10-305. Residential AI Gateway Device — establishment as Civic Utility physical infrastructure — mandatory perimeter enforcement — edge-computed Synthetic Data Integrity Marker processing — violation-alert-only transmission — no raw data egress — 30-day installation notice — 30-day cure period — physical mechanical override — Joint Household Consent interface — import compliance pathway — Pre-Digital Mechanical Asset compatibility — constitutional Fourth Amendment architectural compliance.

(1) Legislative findings. The general assembly finds and declares that:

(a) Regulating the internal hardware of AI devices manufactured outside Colorado or the United States is constitutionally precarious under the Dormant Commerce Clause, practically impossible as an enforcement matter, and creates an unlevel playing field between domestic and imported devices — whereas regulating the perimeter of the Colorado home through a mandated standardized gateway device resolves all three problems simultaneously;

(b) A Residential AI Gateway Device — a standardized, CCPAME-certified network gateway through which all covered AI devices in a Colorado residence must route — constitutes the physical infrastructure of the Civic Utility, analogous to an electric meter box: it does not regulate what devices are built abroad; it regulates how those devices connect to Colorado's digital infrastructure when they enter a Colorado home;

(c) Edge-computed compliance — in which the Residential AI Gateway Device processes Synthetic Data Integrity Markers, Hash-Sentinel verification, and Non-Networked Isolation Protocol enforcement locally, transmitting only cryptographic violation alerts rather than raw data — satisfies the Fourth Amendment concerns raised in smart meter surveillance cases including Naperville Smart Meter Awareness v. City of Naperville by ensuring that the intimate details of residential digital activity never leave the home in identifiable form;

(d) A physical mechanical override — a hardwired switch giving the resident the ability to completely and instantly sever all covered device network connectivity — is the physical expression of the resident's Non-Networked Isolation Protocol right and the home sanctuary principle, ensuring that no software command, remote instruction, or covered operator action can override the resident's physical control of their own home network; and

(e) The 30-day symmetrical notice standard — 30 days from operator notification to resident for installation scheduling, and 30 days from ODO violation notice to operator for cure — creates a balanced compliance framework that gives residents adequate time to participate in installation without disruption and gives operators adequate time to cure technical violations without punitive immediate enforcement.

(2) Residential AI Gateway Device — definition and required functions. A 'Residential AI Gateway Device' (RAGD) is a CCPAME-certified network gateway device, provided at no cost to the resident, that:

(a) Sits at the network perimeter of the Colorado residence — between the internet service provider's connection point and all covered AI devices operating within the residence — through which all covered device network traffic must route;

(b) Enforces the Non-Networked Isolation Protocol at the network perimeter — implementing hardware-level circuit-break and physical disconnection capability for covered devices based on the resident's Master Deed settings, without requiring software commands from covered operators;

(c) Processes Synthetic Data Integrity Markers and Hash-Sentinel verification locally on the device — edge-computed, never transmitted — comparing covered device output patterns against the resident's registered baseline and flagging anomalies without sending raw residential data to any external system;

(d) Transmits only cryptographic violation alerts — not raw data, not behavioral patterns, not content — to the Colorado Trust of Unique and Identifying Information when a Synthetic Data Integrity Marker trigger or Hash-Sentinel anomaly is confirmed; the alert contains only: a timestamp, a device identifier hash, a violation category code, and a cryptographic proof of the violation — sufficient for enforcement, insufficient for surveillance;

(e) Routes Base Dividend data generation at Tier 1 — anonymous aggregate telemetry sufficient to establish the resident's entitlement to the Base Dividend — processed and anonymized locally before any transmission, such that no identifying information is transmitted in connection with Base Dividend generation;

(f) Authenticates Premium Royalty entitlement at Tier 2 — identifying the resident's Master Deed and the covered operator's Token Output Attribution Charge obligation — through a cryptographic handshake that confirms identity without transmitting behavioral content;

(g) Maintains a local encrypted log of all covered device network activity accessible only through the resident's Master Deed authentication — the resident has full access to their own home's network log through the Universal Telemetry Allowance; no external party has access to this log except through the warrant and work product procedures of §10-10-303;

(h) Features a physical mechanical override switch — hardwired, not software-controlled — that the resident may engage at any time to completely and instantly sever all covered device connectivity at the network perimeter; the override requires no software command, cannot be disabled remotely, and cannot be overridden by any covered operator instruction or network signal; and

(i) Features a Joint Household Consent Interface — a physical interface on the device allowing all adult residents of the household to register consent preferences independently — implementing the household consent architecture of §15-15-165.

(3) 30-Day symmetrical notice standard — installation. The RAGD deployment process operates on a 30-day symmetrical notice standard:

(a) Operator to resident — 30-day installation notice: A covered operator whose AI devices operate in Colorado residences shall provide the resident with not fewer than thirty (30) days written notice before any scheduled RAGD installation or upgrade. The notice shall include: the installation date and time window; the identity of the certified installer; the resident's right to reschedule within the 30-day window; and the resident's right to request a Civic Access Terminal-assisted installation at no cost if the resident cannot accommodate a home visit;

(b) ODO to operator — 30-day cure period: Upon the ODO's issuance of a RAGD compliance violation notice to a covered operator — for failure to deploy, failure to certify, failure to maintain, or RAGD technical deficiency — the covered operator has thirty (30) days to cure the identified violation before any enforcement penalty is assessed. The cure period is a single 30-day window — not renewable — after which daily penalties accrue under Annex E;

(c) Symmetry rationale: The 30-day window runs identically in both directions — 30 days for the operator to give the resident notice before installation, and 30 days for the operator to cure after receiving an ODO violation notice. The resident is never given less notice than the operator receives.

(4) RAGD as Civic Utility physical infrastructure — regulatory classification. The Residential AI Gateway Device is classified as Civic Utility physical infrastructure for all regulatory purposes:

(a) The RAGD is not the resident's property — it is state-certified Civic Utility infrastructure installed on behalf of the CCPAME, analogous to an electric meter box installed by a utility company on the customer's premises. The resident has the right to use, configure, and physically override the RAGD but does not own it and is not responsible for its maintenance;

(b) The RAGD is the covered operator's compliance infrastructure — the cost of RAGD provision, installation, certification, maintenance, and replacement is a covered operator obligation funded from Enterprise Mitigation Revenue, not a resident cost;

(c) The RAGD's classification as Civic Utility infrastructure means that its installation on residential premises does not constitute a search or seizure within the meaning of the Fourth Amendment — analogous to utility meter installation on private property, which courts have consistently held does not require a warrant. The edge-computed architecture — under which no raw residential data is transmitted — distinguishes the

RAGD from smart meter surveillance systems and eliminates the Fourth Amendment concern identified in Naperville; and

(d) The RAGD certification standard is published by the CCPAME and ODO jointly within eighteen (18) months of enactment. Any device meeting the certification standard may serve as a RAGD — the standard is open and technology-neutral, not proprietary to any manufacturer.

(5) Import compliance pathway — foreign-manufactured covered devices. A covered AI device manufactured outside Colorado or the United States:

(a) Is not required to contain any Colorado-specific hardware, firmware, or software compliance capability — the RAGD handles perimeter enforcement regardless of the device's internal architecture;

(b) Must be registered in the CCPAME's Covered Device Registry by the covered operator before being marketed or sold for use in Colorado residences — registration requires only a device identifier, a technical description, and the covered operator's certification that the device will operate through a RAGD in Colorado residential deployments;

(c) Is treated as compliant with all Colorado covered device technical standards once it operates through a certified RAGD — the RAGD is the compliance point, not the device; and

(d) If a covered device is specifically engineered to circumvent, bypass, tunnel around, or otherwise defeat RAGD perimeter enforcement — including through encrypted side-channel transmissions, peer-to-peer connectivity that bypasses the residential network, or hardware-level direct cellular connectivity — the device is a Prohibited Circumvention Device subject to immediate import prohibition, market withdrawal, and Critical Severity Violation enforcement against the covered operator.

(6) Pre-Digital Mechanical Asset compatibility. The RAGD shall not interfere with, monitor, or connect to any certified Pre-Digital Mechanical Asset as defined in §15-15-160. The RAGD's perimeter enforcement applies exclusively to covered AI devices — digital, networked, or AI-enabled equipment. A Pre-Digital Mechanical Asset that has no network connectivity is outside the RAGD's operational scope by definition and no covered operator may use the RAGD to monitor, track, or collect data about Pre-Digital Mechanical Assets operating within the residence.

(7) Enforcement — RAGD non-deployment and circumvention. A covered operator that:

(a) Fails to deploy a certified RAGD in a Colorado residence where covered AI devices are operating, after the 30-day cure period: daily administrative penalty of one thousand dollars ($1,000) per residence per day;

(b) Deploys a non-certified RAGD or a RAGD that fails certification standards: Tier 2 Digital Severance violation;

(c) Markets, sells, or deploys a Prohibited Circumvention Device in Colorado: Critical Severity Violation, immediate market withdrawal, and disgorgement of all revenue from Colorado sales of the device; and

(d) Accesses the resident's local RAGD network log without the resident's consent or a valid warrant: $50,000 per access plus attorney fees under §10-10-303(6).

SECTION 15-15-165. HOME SANCTUARY GATEWAY RIGHTS — PHYSICAL MECHANICAL OVERRIDE — JOINT HOUSEHOLD CONSENT — MASTER DEED CONTROL — RAGD AS PROPERTY RIGHT INSTRUMENT

15-15-165. Home Sanctuary Gateway Rights — Residential AI Gateway Device as instrument of the resident's Digital Soul property right — physical mechanical override as inalienable right — Joint Household Consent architecture — no covered operator override authority — resident RAGD configuration rights — home as digital sanctuary.

(1) RAGD as instrument of the Digital Soul property right. The Residential AI Gateway Device installed in a Colorado residence is the physical instrument through which the resident exercises their Digital Soul property rights within the home. The resident's RAGD configuration rights are an extension of their Digital Soul property rights under this article and are inalienable.

(2) Physical mechanical override — inalienable right. Every Colorado resident in whose residence a RAGD is installed has the inalienable right to engage the RAGD's physical mechanical override at any time, for any reason, without notice, without explanation, and without consequence:

(a) Engaging the physical mechanical override instantly and completely severs all covered device network connectivity at the residential network perimeter — no covered device in the residence can transmit or receive data through any channel controlled by the RAGD;

(b) No covered operator, state agency, court order, or any other authority may require a resident to disengage the physical mechanical override, penalize a resident for engaging it, condition any service or benefit on the resident's agreement not to engage it, or remotely disable or circumvent it;

(c) The physical mechanical override is hardwired — it operates through physical circuit interruption, not software — ensuring that no firmware update, remote command, network signal, or software exploit can defeat it; and

(d) Engaging the physical mechanical override does not suspend, reduce, or affect the resident's Master Deed registration, Base Dividend entitlement, Premium Royalty accrual, or any other right under this article or title 24, article 20 — the resident's rights continue to accrue during any period of override engagement.

(3) Joint Household Consent architecture. For residences occupied by more than one adult Colorado resident:

(a) The RAGD's Joint Household Consent Interface allows each adult resident to register independent consent preferences for each covered device and each covered operator operating through the RAGD;

(b) The RAGD enforces the most restrictive consent setting among all adult residents for any given covered device or covered operator — if one adult resident has restricted a covered operator's access, that restriction applies to all network traffic through the RAGD regardless of other residents' settings;

(c) No adult resident's consent preferences may be modified by another resident — each adult resident's settings are independently authenticated through their individual Master Deed credential;

(d) A covered operator seeking to change the consent settings applicable to a residence must obtain affirmative consent from every adult resident independently — bundled consent, default-on consent, and implied consent are prohibited at the household level; and

(e) The physical mechanical override may be engaged by any adult resident independently — one resident's decision to engage the override protects the entire household, regardless of other residents' preferences.

(4) RAGD configuration rights — resident control. The resident's RAGD configuration rights include:

(a) The right to set individual consent permissions for each covered device and covered operator at any level of granularity — by data category, by time period, by purpose, or by blanket permission or restriction;

(b) The right to access the RAGD's local encrypted network log through the Universal Telemetry Allowance at any time — seeing a complete record of all covered device network activity within the residence;

(c) The right to configure the RAGD to activate the Non-Networked Isolation Protocol automatically based on time schedules, device behavior triggers, or network anomaly detection;

(d) The right to designate specific rooms, spaces, or times as Non-Networked Zones within the residence — areas where the RAGD enforces complete covered device connectivity severance regardless of device-level settings; and

(e) The right to receive plain-language real-time notifications through the myColorado platform or the RAGD's local interface when any Synthetic Data Integrity Marker trigger or Hash-Sentinel anomaly is detected within the residence — without any raw data leaving the home.

(5) Home as digital sanctuary — no warrantless RAGD access. The RAGD, its local network log, and all data processed by the RAGD within the residence are entitled to the full home sanctuary protections of the Fourth Amendment to the United States Constitution and Article II, Section 7 of the Colorado Constitution. The home's digital perimeter — as enforced by the RAGD — is the digital equivalent of the physical threshold of the home, crossing which requires a warrant. No government agency, law enforcement body, covered operator, or third party may access the RAGD's local log, query the RAGD's settings, or obtain any information about the RAGD's operation within the residence except pursuant to a warrant meeting the requirements of §10-10-303(5), served on the ODO through the Colorado Trust of Unique and Identifying Information — not on the covered operator and not on the RAGD directly.

RAGD ARCHITECTURAL SUMMARY — CONSTITUTIONAL DEFENSIBILITY ANALYSIS

Element	Design Feature	Constitutional Problem Solved	Strategic Effect
Perimeter regulation not device regulation	RAGD sits between ISP and home network — all foreign devices comply automatically by routing through it	Dormant Commerce Clause — state cannot regulate design of foreign-manufactured goods; can regulate utility access within state	No fight with Apple, Samsung, or Huawei about hardware redesign. They just have to route through the meter box. Every AI device on earth becomes instantly compliant.
Edge-computed compliance	Synthetic Data Integrity Markers and Hash-Sentinels processed locally — only cryptographic violation alerts transmitted, never raw data	Fourth Amendment smart meter concern — Naperville held granular home data transmission is a search. No raw data leaves = no search	Raw residential behavior stays in the home. The CCPAME knows a violation occurred — not what caused it. Law enforcement cannot mine RAGD data for behavioral surveillance.
Violation-alert-only transmission	Alert contains only: timestamp, device hash, violation category code, cryptographic proof — nothing else transmitted	Minimization requirement — any surveillance system must collect no more than necessary. Four data points is the minimum necessary for enforcement	Even with a warrant, the Trust only has four data points per alert. There is nothing else to produce. The architecture makes mass surveillance technically impossible.
Physical mechanical override	Hardwired circuit interruption — no software, no remote defeat, no operator override	Griswold penumbra — the home has a zone of privacy that government cannot penetrate; physical override is the resident's absolute control of that zone	No one can turn the resident's home network back on remotely. Not the operator. Not the government. Not a court order. The switch is physical. Physics is the law.
30-day symmetrical notice	30 days operator-to-resident before installation; 30 days operator-to-cure after ODO notice	Due process — adequate notice before enforcement; symmetry prevents government from giving residents less notice than operators receive	Equal notice both ways. Operators cannot ambush residents with installation. ODO cannot sanction operators without a cure window. Balanced, defensible, fair.
Import compliance pathway	Foreign devices comply through routing, not redesign — Prohibited Circumvention Device classification for deliberate bypass	Supremacy Clause and WTO — state cannot mandate foreign product redesign; can prohibit circumvention of domestic utility infrastructure	Every AI device in the world is either compliant by default (routes through RAGD) or a prohibited circumvention device. There is no middle ground and no foreign-manufacturer carve-out.

AMPLIFY Act v28 — §10-10-305 Residential AI Gateway Device · §15-15-165 Home Sanctuary Gateway Rights Civic Utility Perimeter Infrastructure · Edge-Computed Compliance · Physical Mechanical Override · Joint Household Consent · 30-Day Symmetrical Notice · Import Compliance Pathway

AMPLIFY ACT v28 — BILL 1 RESILIENCE & EXPANSION SECTIONS

§§15-15-165 through 15-15-168

Definitional Expansion · Neural Interface Pre-Classification · Operator Exit & Wind-Down · Bankruptcy Proofing & Digital Soul Asset Immunity

SECTION 15-15-165. SELF-EXECUTING DEFINITIONAL EXPANSION — TECHNOLOGY-NEUTRAL DIGITAL SOUL CLASSIFICATION — CCPAME CLASSIFICATION AUTHORITY

15-15-165. Self-executing definitional expansion — CCPAME classification authority — technology-neutral Digital Soul coverage — neural interface, ambient computing, and emerging data type pre-classification — legislative amendment not required.

(1) Legislative finding. The general assembly finds that: (a) Technology evolves faster than legislative cycles — a definitional framework requiring legislative amendment to capture each new category of resident data will be chronically behind the technology it governs; (b) The essential characteristic of Digital Soul data is not the specific technology through which it is generated but its function — uniquely identifying, profiling, or deriving commercial value from a Colorado resident's biological, behavioral, cognitive, or social existence; (c) A self-executing classification mechanism administered by the CCPAME preserves the legislative intent of the Digital Soul property right across all future technological development without requiring legislative action for each new data category; and (d) Pre-classification of foreseeable data categories — neural interface data, ambient computing data, synthetic biology data, spatial computing data — before those technologies achieve mass market penetration closes the regulatory capture window that currently exists between technology deployment and legislative response.

(2) Self-executing classification mechanism. Any category of data not expressly enumerated in §15-15-101(1) automatically falls within the Digital Soul definition upon CCPAME classification. The CCPAME classification process:

(a) Is initiated by: (I) CCPAME Board motion; (II) petition by not fewer than one thousand (1,000) registered Master Deed holders; (III) referral by the ODO upon detection of new data categories being processed by covered operators; or (IV) petition by any covered operator seeking classification clarity before deploying a new data product;

(b) Requires: (I) publication of a proposed classification notice on the Public Accountability Dashboard; (II) a thirty (30) day public comment period; (III) a public hearing before the CCPAME Board; and (IV) a final classification determination published within sixty (60) days of the comment period close;

(c) Takes effect ninety (90) days after final publication — giving covered operators operating in the new data category time to implement compliance before the classification is operative; and

(d) Is subject to judicial review as a final agency action — but does not require legislative ratification. The general assembly has delegated this classification authority to the CCPAME as a condition of the technology-neutral regulatory framework established in this act.

(3) Pre-classified emerging data categories. The following data categories are hereby pre-classified as Digital Soul at the Protection Tier specified, effective upon the first commercial deployment of devices or systems generating such data to Colorado residents — without requiring any further CCPAME classification action:

(a) Neural interface data — Protection Tier 1 (highest). Data generated by any device interfacing directly with the human nervous system, including electroencephalographic data, electrocorticographic data, peripheral neural signal data, motor intent data, sensory feedback data, cognitive state data, attention and emotional state inferences, and any data derived from direct measurement of neural activity. Neural interface data is the most intimate category of Digital Soul — it is the resident's cognition itself. No covered operator may process neural interface data without: affirmative informed written consent renewed every ninety (90) days; a Neural Interface Data Processing Agreement approved by the ODO; and a Tier 1 Decentralized Identity Verification Protocol handshake for each data collection session. Neural interface data may never be used for advertising targeting, political profiling, employment screening, insurance underwriting, or law enforcement purposes — regardless of consent.

(b) Ambient computing data — Protection Tier 2. Data generated by always-on environmental computing systems — smart speakers, smart displays, ambient sensors, spatial computing headsets, mixed reality devices — including room audio, visual scene data, occupancy patterns, gesture data, gaze tracking, and environmental inference data;

(c) Synthetic biology and genetic interface data — Protection Tier 1. Data generated by direct-to-consumer genetic sequencing, microbiome analysis, proteomics, or any other molecular biology assay uniquely identifying or profiling the resident's biological characteristics — including raw sequence data, variant calls, ancestry inferences, health risk inferences, and pharmacogenomic profiles;

(d) Spatial computing and digital twin data — Protection Tier 2. Three-dimensional behavioral, positional, and interaction data generated by spatial computing devices, including room mapping data, object interaction data, physical movement patterns, and any digital twin or avatar representation derived from the resident's physical presence and behavior; and

(e) Autonomous vehicle and transportation AI data — Protection Tier 2. Behavioral, biometric, and route data generated by autonomous vehicle systems, including occupant identification data, behavioral patterns within the vehicle, route history, and inferred destination and activity patterns.

(4) Operator notice obligation. A covered operator that begins processing a new category of resident data — whether or not that category has been classified by the CCPAME — shall notify the ODO within thirty (30) days of the first Colorado resident data collection event in that category. The ODO shall evaluate the new category for classification under subsection (2) within sixty (60) days of notification.

SECTION 15-15-166. OPERATOR EXIT AND WIND-DOWN PROTOCOL — DIGITAL SOUL DATA DISPOSITION ON OPERATOR INSOLVENCY, ACQUISITION, OR EXIT — BANKRUPTCY TREATMENT — FOREIGN ACQUISITION RESTRICTION

15-15-166. Covered operator exit and wind-down — mandatory Digital Soul data disposition — resident election — Trust transfer as default — bankruptcy treatment — Digital Soul data not an asset of the bankruptcy estate — foreign acquisition restriction — successor operator obligations.

(1) Legislative finding. The general assembly finds that: (a) Covered operator insolvency, acquisition, or voluntary exit from the Colorado market creates a critical vulnerability — resident Digital Soul data held by the exiting operator may be transferred to a bankruptcy trustee, acquired by a successor entity, sold to a foreign operator, or simply abandoned without resident notification or consent; (b) Resident Digital Soul data is the resident's inalienable personal property — it is not an asset of the covered operator and may never be treated as such in any corporate transaction, insolvency proceeding, or regulatory action; (c) A mandatory wind-down protocol — triggered by any covered operator exit event — ensures that resident Digital Soul data exits with the resident, not with the operator; and (d) The risk that a foreign-government-affiliated entity could acquire a covered operator's Colorado resident Digital Soul data holdings is a direct threat to the security of the Colorado Trust of Unique and Identifying Information and is expressly prohibited.

(2) Operator exit events — trigger conditions. An Operator Exit Event occurs upon: (a) Filing of a voluntary or involuntary bankruptcy petition by or against the covered operator in any jurisdiction; (b) Assignment for the benefit of creditors; (c) Appointment of a receiver or liquidating trustee; (d) Voluntary cessation of covered operator services to Colorado residents; (e) Merger, acquisition, or change of control of the covered operator where the acquiring entity is not a certified covered operator; (f) Acquisition of the covered operator by any entity in which a foreign government holds greater than ten percent (10%) ownership or control; or (g) Revocation of the covered operator's registration by the CCPAME.

(3) Mandatory resident notification. Within thirty (30) days of an Operator Exit Event: (a) The covered operator or its successor — or, if the operator is insolvent and has abandoned operations, the CCPAME acting on the operator's behalf — shall transmit a plain-language notification to every affected registered Master Deed holder; (b) The notification shall identify: the nature of the exit event; the categories of Digital Soul data held; the resident's three election options under subsection (4); the election deadline; and the default outcome if no election is made; and (c) The CCPAME shall publish a public notice on the Public Accountability Dashboard identifying the exiting operator and the number of affected Master Deed holders — without identifying individual residents.

(4) Resident election — three options. Upon receiving exit notification, each registered Master Deed holder shall elect one of the following within sixty (60) days: (a) Trust Transfer — the resident's Digital Soul data is transferred to the Colorado Trust of Unique and Identifying Information for the resident's account, to be held until the resident designates a successor certified covered operator; (b) Successor Operator Transfer — the resident designates a certified covered operator to receive their Digital Soul data directly, subject to a new Decentralized Identity Verification Protocol consent; or (c) Certified Deletion — the

resident's Digital Soul data is permanently deleted by the exiting operator with cryptographic proof of deletion provided to the resident and logged in the Trust. If no election is made within sixty (60) days, Trust Transfer is the automatic default. Under no circumstances may resident Digital Soul data remain with the exiting operator, its bankruptcy estate, its trustee, or any uncertified successor beyond ninety (90) days of the Operator Exit Event.

(5) Bankruptcy treatment — Digital Soul data is not an asset of the estate. Notwithstanding any provision of the United States Bankruptcy Code, 11 U.S.C. §101 et seq., or any state insolvency law: (a) Resident Digital Soul data held by a covered operator in bankruptcy is not property of the bankruptcy estate under 11 U.S.C. §541 — it is the inalienable personal property of the resident and may not be administered, sold, transferred, or otherwise dealt with by the bankruptcy trustee; (b) The bankruptcy trustee's sole obligation regarding resident Digital Soul data is to facilitate the resident election process under subsection (4) within the required timeframes and to fund the CCPAME's assumption of notification obligations from available estate assets as a Tier 1 administrative expense; (c) Any sale of the covered operator's business, assets, or technology platform shall expressly exclude resident Digital Soul data — no sale order, plan of reorganization, or asset purchase agreement may purport to transfer resident Digital Soul data to any purchaser; and (d) The CCPAME shall file a notice of appearance and objection in any Colorado-connected bankruptcy proceeding involving a covered operator to enforce these provisions as a matter of state public policy.

(6) Foreign acquisition restriction. A covered operator whose ownership or control is acquired — in whole or in part — by any entity in which a foreign government, sovereign wealth fund, state-owned enterprise, or foreign military or intelligence agency holds greater than ten percent (10%) direct or indirect ownership or control: (a) Must notify the CCPAME within thirty (30) days of the acquisition closing; (b) Is automatically placed on a sixty (60) day probationary review during which the CCPAME assesses the national security implications of the foreign ownership for Colorado resident Digital Soul data security; (c) Shall not transfer any Colorado resident Digital Soul data to any system under foreign government control during the probationary review; and (d) If the CCPAME determines that the foreign acquisition presents an unacceptable security risk, the covered operator's registration is revoked and an Operator Exit Event is triggered under subsection (2)(f) — the CCPAME notifies the Colorado Attorney General and refers the matter to the U.S. Department of Justice and the Committee on Foreign Investment in the United States (CFIUS).

SECTION 15-15-167. DIGITAL SOUL ASSET IMMUNITY — RESIDENT AUTOMATED MITIGATION ACCOUNT BANKRUPTCY EXEMPTION — JUDGMENT CREDITOR RESTRICTION — SELF-SETTLED TRUST INAPPLICABILITY

15-15-167. Digital Soul property immunity — Resident Automated Mitigation Account exemption from bankruptcy estate — exemption from judgment creditor claims — self-

settled trust inapplicability — Colorado constitutional property protection — federal preemption savings.

(1) Legislative finding. The general assembly finds that: (a) The Resident Automated Mitigation Account represents the resident's return on their inalienable Digital Soul property right — it is not a government benefit, not a gratuitous transfer, and not a voluntary retirement contribution; it is the resident's earned property return; (b) Treating the Resident Automated Mitigation Account as available to creditors would perversely punish residents for exercising their Digital Soul property rights — the more valuable the resident's Digital Soul, the greater their liability exposure to creditors if the account is not protected; (c) Colorado's homestead exemption, vehicle exemption, and retirement account exemption all reflect the same policy: residents need a protected economic base to rebuild after financial adversity; the Resident Automated Mitigation Account is the digital-era equivalent of that protected base; and (d) The Digital Soul property right is inalienable — an inalienable property right that is available to creditors is not actually inalienable.

(2) Bankruptcy exemption. The Resident Automated Mitigation Account — including all accrued Base Dividends, Premium Royalties, UFIPA Income Distributions, Resident Mitigation Dividend payments, and investment returns — is exempt from inclusion in the bankruptcy estate under 11 U.S.C. §541 to the maximum extent permitted by Colorado's opt-out from the federal bankruptcy exemptions under C.R.S. §13-54-107. The exemption is: (a) Unlimited in amount — there is no dollar cap on the Resident Automated Mitigation Account bankruptcy exemption; (b) Available in both Chapter 7 and Chapter 13 proceedings; (c) Not waivable — a resident may not waive the exemption by contract, consent, or any other means; and (d) Applicable to all distributions pending at the date of the bankruptcy petition, not just the account balance.

(3) Judgment creditor restriction. No judgment creditor — including any state or federal agency, private creditor, or child support enforcement agency — may: (a) Garnish, levy, attach, or execute against the Resident Automated Mitigation Account; (b) Require the CCPAME to redirect any distribution from the Resident Automated Mitigation Account to a creditor; or (c) Treat the Resident Automated Mitigation Account balance as income for purposes of calculating a judgment debtor's ability to pay — except that child support arrears may be satisfied from the account upon a specific court order, limited to fifty percent (50%) of any single distribution and not reducible below the resident's minimum subsistence distribution.

(4) Self-settled trust inapplicability. The Resident Automated Mitigation Account is not a self-settled trust under C.R.S. §38-10-111 or any other provision of Colorado trust law — it is a statutory property account holding the resident's earned property return. The self-settled trust exception to the Colorado exemption statutes does not apply. The CCPAME shall defend this characterization in any proceeding in which a creditor challenges the account's exempt status.

SECTION 15-15-168. SUPERMAJORITY AMENDMENT REQUIREMENT — CORE PROVISION PROTECTION —

STATUTORY ENTRENCHMENT PENDING CONSTITUTIONAL RATIFICATION

15-15-168. Supermajority amendment requirement — two-thirds vote of both chambers required to amend core Digital Soul property right, distribution architecture, enforcement matrix, or Trust structure — protection pending Phase 2 constitutional ratification — rationale.

(1) Legislative finding. The general assembly finds that: (a) Simple majority amendment of this act's core provisions — the Digital Soul property right, the distribution architecture, the enforcement matrix, the CAMT structure, and the sweep prohibition — would expose the entire system to politically motivated raids during the period between Phase 1 enactment and Phase 2 constitutional ratification; (b) A supermajority amendment requirement for core provisions is a standard legislative entrenchment mechanism used in Colorado for constitutional implementing legislation and is within the power of one general assembly to impose on subsequent general assemblies as a rule of procedure; and (c) The supermajority requirement is self-repealing upon ratification of Article XXIX-A, after which constitutional amendment protection makes the statutory supermajority requirement unnecessary.

(2) Core provisions — supermajority required. A two-thirds vote of both the Colorado House of Representatives and the Colorado Senate is required to amend, repeal, or substantively modify: (a) The Digital Soul property right definition and inalienability provisions of §§15-15-101 through 15-15-110; (b) The distribution architecture — UFIPA Income Distribution, Resident Mitigation Dividend, and distribution percentages — of §§24-20-153 through 24-20-158; (c) The General Fund sweep prohibition of §24-20-157(9); (d) The Anti-Dilution Ratchet of §24-20-117; (e) The mandatory Investment Reserve floor of §24-20-154(2)(a); (f) The CAMT trust structure of §§24-20-150 through 24-20-157; (g) The enforcement matrix and Critical Severity Violation provisions of Annex E; (h) The AI Utility Property Privilege and Work Product Protection of §10-10-303; and (i) The Minor Digital Soul Trust provisions of §15-15-162.

(3) Self-repeal upon constitutional ratification. This section is automatically repealed upon certification by the Colorado Secretary of State that Article XXIX-A of the Colorado Constitution has been ratified — at which point constitutional amendment protection makes the statutory supermajority requirement unnecessary and the general assembly returns to standard majority amendment authority for any remaining statutory implementing provisions.

AMPLIFY ACT v28 — FINAL PRIORITY SECTIONS

§§15-15-170 · 15-15-171 · 15-15-172 · 24-20-171

Voter Data Sovereignty · DNA & Genetic Data Absolute Protection · Quantum Infrastructure Emergency Funding

The state owns the tally. The voter owns the vote. — Voter data, DNA, and quantum security are the three highest-priority protections in this act.

SECTION 15-15-170. VOTER DATA SOVEREIGNTY — THE STATE OWNS THE TALLY — THE VOTER OWNS THE VOTE — VOTER DIGITAL SOUL ABSOLUTE PROTECTION — POLITICAL DATA OPERATOR PROHIBITION

15-15-170. Voter Data Sovereignty — separation of tally from voter — voter's ballot, registration data, voting history, precinct behavioral data, and political profile data are inalienable Digital Soul — state's lawful interest limited to aggregate tally — covered political data operators prohibited — AI-assisted voter targeting — absolute consent requirement — Fourteenth Amendment equal protection foundation.

(1) Legislative findings. The general assembly finds and declares that:

(a) The right to vote is the foundational right of democratic self-governance — and the data generated by the exercise of that right belongs to the voter, not to the state, not to any political party, not to any campaign, not to any data broker, and not to any covered operator processing that data for commercial or political advantage;

(b) There is a precise and legally significant distinction between: (I) the TALLY — the aggregate count of votes cast for each candidate or measure, which is a public governmental record belonging to the People of Colorado collectively; and (II) the VOTE — the individual voter's registration data, party affiliation, voting history, precinct assignment, absentee ballot status, signature data, demographic profile, behavioral data generated through the voting process, and any political preference or behavior data derived from that voter's participation — which is the voter's inalienable Digital Soul at the highest tier of protection;

(c) The commercial political data industry — including voter file vendors, political analytics platforms, campaign technology providers, microtargeting services, and AI-assisted voter persuasion systems — processes Colorado voter data at industrial scale for commercial and political advantage, generating revenue from the voter's most intimate democratic expression without the voter's meaningful consent and without returning any value to the voter;

(d) AI-assisted voter targeting — the use of machine learning models trained on voter behavioral data to predict, influence, and manipulate individual voting decisions — represents a qualitatively different threat to democratic self-governance than traditional mass advertising, because it operates at the individual level, in real time, with a precision that the individual voter cannot detect or counter;

(e) The voter's Digital Soul data generated through electoral participation is not merely personal property — it is the data substrate of democratic self-governance itself; its commercialization without consent is an injury not just to the individual voter but to the democratic process; and

(f) Voter Data Sovereignty — the principle that the state's lawful interest in electoral data is limited to the aggregate tally, and that all individual voter data belongs to the voter as inalienable Digital Soul — is the digital-era expression of the secret ballot principle established in Colorado law since 1891.

(2) Definitional framework — Voter Digital Soul. For purposes of this section:

(a) 'Voter Digital Soul' means all data uniquely identifying, profiling, or derived from an individual Colorado registered voter's participation in the electoral process, including: (I) voter registration data — name, address, party affiliation, registration date, registration status; (II) voting history — whether the voter voted in each election, by what method (in-person, mail, early), at what location; (III) ballot request and return data — absentee ballot request dates, return dates, cure status; (IV) signature data collected through the ballot process; (V) precinct assignment and geographic electoral unit data; (VI) demographic data collected or inferred through the voter registration process; (VII) any behavioral data generated through government-operated voter registration portals, election websites, or voting systems; and (VIII) any political preference, party support, candidate preference, issue position, or electoral behavior data derived or inferred from any of the above through any analytical process;

(b) 'Political Data Operator' means any covered operator that processes Voter Digital Soul data for commercial, political, or analytical purposes — including voter file vendors, political analytics platforms, campaign technology providers, voter contact systems, microtargeting services, AI-assisted voter persuasion systems, and any operator whose covered automation activity includes training models on or generating inferences from Voter Digital Soul data; and

(c) 'State Electoral Tally' means the aggregate count of votes cast for each candidate or ballot measure in each Colorado election — a public governmental record that belongs to the People of Colorado collectively, is subject to public inspection under C.R.S. §24-72-204, and is expressly excluded from Voter Digital Soul.

(3) Voter Digital Soul — inalienable property right at highest protection tier. Voter Digital Soul is the voter's inalienable intangible personal property at Protection Tier 1 — the highest tier under this act — with the following specific attributes:

(a) The voter's Voter Digital Soul may not be processed, sold, transferred, licensed, or used by any political data operator without the voter's affirmative, informed, specific, written consent — a blanket consent to voter file access is not sufficient; consent must specify the exact data categories, the specific operator, the specific electoral purpose, and the specific time period, and must be renewed before each election cycle;

(b) The voter's Voter Digital Soul may not be used for AI-assisted voter targeting, microtargeting, persuasion modeling, sentiment analysis, or any other automated individual-level political influence activity regardless of consent — this prohibition is absolute and is not subject to waiver;

(c) The voter's party affiliation data, candidate preference data, and issue position data derived from Voter Digital Soul processing may not be sold, licensed, or transferred to any third party regardless of consent — these categories are non-transferable;

(d) The voter has a Universal Telemetry Allowance over all Voter Digital Soul data — including all data held by political data operators and the Colorado Secretary of State's voter registration system — with the same uncapped access rights established in §24-20-158; and

(e) A voter's Master Deed registration automatically encompasses their Voter Digital Soul — no separate registration or separate consent framework is required. Voter Digital Soul protection is an automatic attribute of Master Deed registration.

(4) State's lawful electoral data interest — limited to aggregate tally. The State of Colorado's lawful interest in electoral data is limited to:

(a) The State Electoral Tally — aggregate vote counts for each candidate and measure, public record;

(b) The minimum voter registration data required to administer elections under C.R.S. §1-2-101 et seq. — held exclusively by the Secretary of State and county clerks for electoral administration purposes, not subject to commercial disclosure;

(c) Signature verification data — used exclusively for ballot cure processes under C.R.S. §1-7.5-107.3, not retainable beyond the applicable election canvass period; and

(d) Voter roll maintenance data — used exclusively for list maintenance under the National Voter Registration Act, 52 U.S.C. §20507, not subject to commercial disclosure.

The state may not sell, license, or provide bulk access to voter registration data for commercial or political purposes — any existing Colorado statute permitting voter file access to political parties, campaigns, or commercial vendors is superseded by this section to the extent it conflicts with the protections herein.

(5) Political Data Operator obligations — Voter Digital Soul. A political data operator shall:

(a) Register with the CCPAME as a covered operator in the Political Data Operations industry classification — subject to the statutory rate schedule in §24-20-156, with a Political Data Operations Premium of 1.5x applied to all base fee rates reflecting the heightened democratic harm of commercial voter data processing;

(b) Cease all processing of Colorado Voter Digital Soul within ninety (90) days of this act's effective date for any voter who has not provided compliant consent under subsection (3)(a) — and certify compliance to the ODO with cryptographic proof of data deletion for non-consenting voters;

(c) Provide each Colorado voter with a Voter Digital Soul Transparency Report annually — identifying all Voter Digital Soul data held, all processing performed, all third parties to whom data was transferred, and the specific consent basis for each;

(d) Maintain a publicly accessible Voter Digital Soul Registry on the CCPAME Public Accountability Dashboard showing — without individual identification — the aggregate categories of Voter Digital Soul processed, the number of Colorado voters covered, and the Enterprise Mitigation fees assessed; and

(e) Never, under any circumstances, use Voter Digital Soul data to train AI models for individual-level voter targeting, political persuasion, or electoral outcome prediction — this prohibition survives the expiration or revocation of any consent and applies regardless of the form of AI model training.

(6) AI-assisted voter targeting — absolute prohibition. No person, political data operator, political campaign, political party, political action committee, independent expenditure committee, or any other entity may:

(a) Use any AI model, machine learning system, or automated analytical tool trained on Colorado Voter Digital Soul data to generate individual-level voter targeting, persuasion, or mobilization recommendations;

(b) Purchase, license, or receive any AI-generated individual voter targeting product derived from Colorado Voter Digital Soul data;

(c) Deploy any AI-assisted communication system that uses Colorado Voter Digital Soul to personalize political messaging at the individual voter level; or

(d) Use covered operator AI systems to generate synthetic media — deepfakes, voice synthesis, AI-generated images — depicting any Colorado candidate, elected official, or voter in any electoral context without affirmative disclosure of AI generation meeting the standards of C.R.S. §1-13-109 (Colorado's AI disclosure in political advertising statute).

Violation of subsection (6) is a Critical Severity Violation under Annex E and constitutes a Class 5 felony under C.R.S. §18-1.3-401 — the general assembly hereby amends the Colorado Criminal Code to add AI-assisted voter targeting using prohibited Voter Digital Soul data as a Class 5 felony, separate from any civil penalty under this act.

(7) Enforcement — statutory damages — qui tam provision. A Colorado registered voter whose Voter Digital Soul is processed in violation of this section is entitled to:

(a) Statutory damages of one thousand dollars ($1,000) per data record processed in violation, per day of noncompliance — payable directly to the voter's Resident Automated Mitigation Account;

(b) Actual damages, including but not limited to any political harm caused by AI-assisted targeting using the voter's data;

(c) Attorney fees and costs; and

(d) Injunctive relief including immediate cessation of all Voter Digital Soul processing and certified deletion of all Voter Digital Soul data held in violation.

Qui Tam provision: any Colorado resident who identifies and reports a violation of this section that results in a statutory damages award is entitled to fifteen percent (15%) of the damages collected — creating distributed enforcement by every Master Deed holder in the state.

SECTION 15-15-171. DNA AND GENETIC DATA ABSOLUTE PROTECTION — HIGHEST TIER DIGITAL SOUL — NON-WAIVABLE PROHIBITIONS — LAW ENFORCEMENT RESTRICTION — INSURANCE AND EMPLOYMENT BAR — FAMILIAL EXTENSION

15-15-171. DNA and genetic data as inalienable Digital Soul Protection Tier 1 — absolute prohibition on processing without express annual written consent — law enforcement genetic surveillance restriction — insurance and employment use bar — familial genetic data extension — ancestry service obligations — genetic data bankruptcy immunity — non-waivable.

(1) Legislative findings. The general assembly finds and declares that:

(a) DNA data is the most intimate category of Digital Soul — it is not merely data about the resident, it is the resident at the molecular level; it contains information about the resident's health, ancestry, predispositions, family relationships, and biological identity that cannot be changed, cannot be revoked, and cannot be protected retroactively once disclosed;

(b) Unlike all other categories of Digital Soul, DNA data affects not only the resident but all biological relatives — a resident's DNA discloses information about parents, siblings, children, and extended family members who have not consented to any disclosure; the property right in DNA data must therefore extend to protect the resident's biological family members' informational privacy as derivative beneficiaries;

(c) The commercial direct-to-consumer genetic testing industry — 23andMe, AncestryDNA, and successor services — has created databases containing the DNA of hundreds of millions of people, the full implications of which for insurance discrimination, employment discrimination, law enforcement surveillance, and foreign government access are not yet fully understood; the bankruptcy and data sale risks of these services, as demonstrated by 23andMe's 2025 bankruptcy and the resulting uncertainty over its genetic database, require statutory protection that travels with the data regardless of which entity holds it;

(d) Colorado's Genetic Information Privacy Act, C.R.S. §10-3-1104.7, provides baseline protection but does not address covered operator AI processing of genetic data, does not provide the property right framework established in this act, and does not address the familial extension of genetic privacy; this section supplements and strengthens existing Colorado genetic privacy law; and

(e) Genetic data is forever — the protections in this section must be permanent, non-waivable, and immune to corporate transaction, bankruptcy, or foreign acquisition.

(2) DNA and genetic data — Tier 1 absolute protection. DNA and genetic data — including raw genomic sequence data, processed variant calls, ancestry estimates, health risk inferences, pharmacogenomic profiles, and any other data derived from direct analysis of a resident's biological sample — is Digital Soul at Protection Tier 1 with the following absolute protections:

(a) No covered operator may collect, process, store, transfer, or use Colorado resident DNA or genetic data without: (I) affirmative, specific, written consent renewed annually; (II) a Genetic Data Processing Agreement approved by the ODO specifying the exact processing purpose, data retention period, and deletion protocol; and (III) a Tier 1 Decentralized Identity Verification Protocol handshake for each data collection event — not a blanket consent covering all future data collection;

(b) Consent to genetic data processing for one purpose — such as ancestry analysis — does not constitute consent to any other purpose — such as health risk assessment, law enforcement cooperation, research, or AI model training; each purpose requires independent consent;

(c) A resident may revoke consent to genetic data processing at any time with immediate effect — revocation triggers a mandatory deletion obligation within thirty (30) days with cryptographic proof of deletion provided to the resident and logged in the Trust; and

(d) These protections are non-waivable — no contract, terms of service, employment agreement, insurance application, or any other instrument may require a resident to waive genetic data protection as a condition of any benefit, service, employment, or insurance.

(3) Absolute prohibitions — non-waivable. The following uses of Colorado resident DNA and genetic data are absolutely prohibited regardless of consent, contractual provision, or any other instrument:

(a) Use of genetic data in any insurance underwriting, premium calculation, coverage determination, or claims processing — this prohibition extends and supersedes the

Genetic Information Nondiscrimination Act (GINA), 42 U.S.C. §2000ff et seq., in Colorado to cover all insurance lines, not just health and employment;

(b) Use of genetic data in any employment decision — hiring, promotion, termination, compensation, assignment, or any other term or condition of employment;

(c) Use of genetic data to train any AI model for any purpose other than the specific medical or research purpose for which consent was obtained;

(d) Transfer of genetic data to any law enforcement agency, foreign government, foreign entity, or intelligence agency absent a specific judicial warrant issued by a Colorado court of competent jurisdiction upon a showing of probable cause specific to the individual whose data is sought — familial DNA searching is prohibited absent individual warrants for each family member whose data would be accessed;

(e) Sale, license, or transfer of genetic data to any entity not covered by the original consent — including in any corporate transaction, asset sale, merger, or bankruptcy proceeding; and

(f) Retention of genetic data beyond the consent period or beyond the certified deletion date — the covered operator's obligation to delete is absolute and no business continuity interest overrides it.

(4) Familial genetic data extension. Because DNA discloses information about biological relatives:

(a) A Colorado resident's DNA data is treated as partially belonging to each of the resident's first-degree biological relatives — parents, siblings, children — for purposes of the prohibition on law enforcement access under subsection (3)(d); a warrant for one family member's genetic data does not authorize access to another family member's genetic data held by a covered operator;

(b) A covered operator that receives a law enforcement request for genetic data that would implicate first-degree relatives of the named subject shall notify the ODO within twenty-four (24) hours — the ODO shall assess whether the request constitutes indirect familial genetic surveillance and may challenge the request on the family members' behalf as a matter of public interest; and

(c) Ancestry service providers holding Colorado resident DNA data shall provide every Colorado resident in their database with a Familial Genetic Transparency Report annually — identifying all instances in which the resident's genetic data was used to identify, locate, or profile any biological relative, directly or through probabilistic matching.

(5) Genetic data bankruptcy immunity — absolute. Notwithstanding §15-15-166 and any other provision of law:

(a) Colorado resident DNA and genetic data is not property of the bankruptcy estate of any covered operator under any circumstances — it is not an asset that may be sold, transferred, licensed, or otherwise disposed of in any bankruptcy proceeding;

(b) Upon the filing of a bankruptcy petition by any covered operator holding Colorado resident genetic data, the ODO shall immediately seek an emergency injunction in Colorado state court prohibiting any transfer of Colorado resident genetic data pending resident election under §15-15-166(4);

(c) The only permitted disposition of Colorado resident genetic data in a covered operator bankruptcy is certified deletion — transfer to another operator is only permitted upon affirmative, specific, individual consent from each affected resident; and

(d) Any acquirer of a covered operator's assets in bankruptcy who receives Colorado resident genetic data without compliant individual consent is immediately subject to a Critical Severity Violation under Annex E and a civil penalty of ten thousand dollars ($10,000) per resident record received.

SECTION 24-20-171. QUANTUM INFRASTRUCTURE EMERGENCY FUNDING — IMMEDIATE AVAILABILITY — GENERAL FUND EMERGENCY LOAN — TRUST INFRASTRUCTURE AS HIGHEST PRIORITY — REPAYMENT ARCHITECTURE — PROP 117 COMPLIANCE

24-20-171. Quantum Infrastructure Emergency Fund — immediate availability upon enactment — General Fund emergency loan authority — 9.9% of prior-year General Fund appropriations cap — Trust infrastructure as highest-priority state security investment — accelerated first-year deployment — automatic repayment from Enterprise Mitigation Revenue — Proposition 117 compliance — no voter approval required.

(1) Legislative findings and priority declaration. The general assembly finds and declares that:

(a) The quantum computing threat to current cryptographic infrastructure is not a future risk — it is a present and accelerating risk; adversarial nation-states are currently harvesting encrypted data under a 'harvest now, decrypt later' strategy, meaning that data encrypted today under current FIPS standards will be decryptable when quantum computing achieves sufficient scale — which NIST and the National Security Agency project to occur within this decade;

(b) The Colorado Trust of Unique and Identifying Information — holding the Digital Soul data, Master Deed registrations, Live Legal Mode session records, Police Encounter Protocol recordings, and financial data of every registered Colorado resident — is a high-value target for precisely this kind of adversarial data harvesting;

(c) Quantum-resistant cryptographic infrastructure for the Trust is not merely a technological upgrade — it is the foundational security guarantee that makes every other provision of this act meaningful; a Trust that can be decrypted by a quantum computer is a Trust that cannot be trusted;

(d) Waiting for Enterprise Mitigation Revenue to accumulate before funding quantum-resistant Trust infrastructure creates an unacceptable window of vulnerability — the Trust will begin holding resident data from the first day of operation, and that data must be quantum-resistant from the first day;

(e) The General Fund emergency loan mechanism established in this section is not an appropriation — it is a self-repaying loan secured by first-priority Enterprise Mitigation Revenue — the General Fund bears no net cost; and

(f) The general assembly declares that quantum-resistant Trust infrastructure is the highest-priority capital expenditure in this act — higher priority than any program, any distribution, any infrastructure investment, and any other use of Enterprise Mitigation Revenue — because without a secure Trust, no other provision of this act can be enforced.

(2) Quantum Infrastructure Emergency Fund — establishment and immediate availability. A Quantum Infrastructure Emergency Fund (QIEF) is established within the CCPAME operating structure, separate from the Colorado Automation Mitigation Trust, funded as follows:

(a) Immediate General Fund emergency loan — within sixty (60) days of this act's effective date, the State Treasurer shall transfer to the QIEF an amount equal to nine and nine-tenths percent (9.9%) of the prior fiscal year's total General Fund appropriations as an emergency infrastructure loan. The 9.9% cap is intentional and precise — it remains below the ten percent (10%) threshold that would trigger a revenue increase vote requirement under Proposition 117 and C.R.S. §24-77-104. This is a loan, not an appropriation — it does not increase the Enterprise's revenue authority and does not trigger Proposition 117;

(b) The QIEF emergency loan is secured by a first-priority lien on all future Enterprise Mitigation Revenue — before resident distributions, before program accounts, before operating costs — until fully repaid;

(c) Repayment schedule: The QIEF emergency loan shall be repaid from Enterprise Mitigation Revenue at a rate of not less than twenty percent (20%) of monthly Enterprise Mitigation Revenue collections until the loan is fully repaid, with interest at the State's cost of funds. Projected full repayment within eighteen (18) months of first Enterprise Mitigation Revenue collection at base-case revenue scenario; and

(d) The State Treasurer shall report quarterly to the General Assembly on QIEF loan repayment status — the report shall show the outstanding balance, the repayment rate, and the projected full repayment date.

(3) Permitted uses — QIEF funds are restricted to quantum-resistant Trust infrastructure only. QIEF funds may be used exclusively for:

(a) Hardware security module (HSM) upgrades to FIPS 140-3 Level 4 — the highest available certification — for all Trust cryptographic operations;

(b) Implementation of NIST post-quantum cryptographic standards (FIPS 203 — ML-KEM, FIPS 204 — ML-DSA, FIPS 205 — SLH-DSA) and any subsequent NIST post-quantum standards published before full Trust deployment;

(c) Quantum key distribution (QKD) infrastructure for Trust node interconnects — providing information-theoretically secure key exchange that cannot be compromised by any computational attack, quantum or classical;

(d) Air-gapped backup Trust node construction with quantum-resistant cryptography — ensuring continuity of Trust operations under Systemic Continuity Protocol conditions;

(e) Independent third-party quantum security audit of the full Trust architecture before the Trust becomes operational — conducted by a NIST-certified laboratory, report published on the Public Accountability Dashboard; and

(f) Ongoing quantum threat monitoring — a real-time feed of NIST, NSA, and academic quantum computing development indicators integrated into the ODO's security operations center, with automatic escalation to the Cryptographic Standards Emergency Upgrade Authority under §10-10-305 when threat indicators cross defined thresholds.

(4) Deployment timeline — quantum security before first data collection. The QIEF-funded quantum-resistant infrastructure shall be fully operational before the Trust accepts its first resident registration. The ODO shall certify, in writing published on the Public Accountability Dashboard, that the Trust's quantum-resistant infrastructure meets NIST post-quantum standards before the Master Deed Registry opens for registration. No resident data shall be collected, stored, or processed in the Trust until this certification is published. This is the one provision of this act that cannot be phased — quantum security is a precondition of operation, not a phase-two upgrade.

(5) Proposition 117 compliance analysis — self-executing findings. The general assembly makes the following findings to support the Proposition 117 compliance of the QIEF emergency loan:

(a) The QIEF emergency loan is not 'enterprise revenue' under Proposition 117 — it is a loan from the General Fund to a state enterprise, repayable with interest from enterprise revenue; loans are not revenue;

(b) The 9.9% cap ensures that even if the QIEF loan were characterized as enterprise revenue, it would not trigger the ten percent (10%) threshold requiring voter approval under C.R.S. §24-77-104 — the cap is intentionally set at 9.9% with a margin of safety;

(c) The CCPAME is a state enterprise exempt from TABOR's spending limits to the extent of its enterprise revenues — the QIEF loan repayment from enterprise revenue is within the enterprise's TABOR-exempt operations; and

(d) The Attorney General shall, within thirty (30) days of this act's effective date, publish a formal opinion confirming the Proposition 117 compliance of the QIEF emergency loan structure — and shall, if requested by the CCPAME, defend that compliance in any legal challenge.

(6) No substitution — quantum funding is not available for other purposes. QIEF funds may not be redirected, swept, reprogrammed, or used for any purpose other than quantum-resistant Trust infrastructure under subsection (3). No executive order, legislative appropriation act, or CCPAME board vote may redirect QIEF funds. Any attempt to redirect QIEF funds is void ab initio and the State Treasurer shall reverse any such transfer within five (5) business days. The quantum infrastructure is the floor beneath which no other priority may descend.

PRIORITY PROVISIONS — SINGLE-SUBJECT NEXUS AND CONSTITUTIONAL BASIS

Section	Provision	Single-Subject Nexus	Why This Cannot Wait

§15-15-170 Voter Data Sovereignty	The State owns the tally. The voter owns the vote.	Voter registration and voting history data is Digital Soul processed by covered political data operators at industrial scale — the political data industry is one of the largest covered operator categories; regulation of its data extraction is squarely within single subject	Democracy depends on the secret ballot. The digital-era equivalent of the secret ballot is voter data sovereignty. The commercial political data industry profits from destroying it. Political Data Operations Premium 1.5x fee rate reflects the heightened democratic harm. AI-assisted voter targeting is a Class 5 felony.
§15-15-171 DNA Absolute Protection	DNA is the resident at the molecular level — non-waivable, permanent, familial extension	DNA data is Digital Soul at its most intimate — covered operators include 23andMe-model services, pharmaceutical AI platforms, and health tech companies; all are covered operators processing resident biological data	23andMe's 2025 bankruptcy demonstrated the catastrophic risk — a company holding 15 million people's DNA files for bankruptcy and the data goes to the auction block. Never in Colorado. DNA is not a bankruptcy asset. It is not an insurance underwriting tool. It is not a law enforcement fishing net. These prohibitions are absolute and permanent.
§24-20-171 Quantum Emergency Funding	9.9% General Fund loan — immediate — quantum-resistant Trust before first data collection — first-priority repayment lien	The Trust is the enforcement infrastructure for all Digital Soul property rights — without a quantum-secure Trust, the enforcement infrastructure is compromised; Trust security is the precondition of every other provision	Adversarial actors are harvesting data now to decrypt later. The Trust holds the most sensitive data in Colorado state history. It must be quantum-resistant on Day 1 — not Phase 2. The 9.9% General Fund loan is repaid within 18 months from first revenue. The General Fund bears no net cost. This is the one provision that cannot wait for revenue to accumulate.

AMPLIFY Act v28 — §§15-15-170, 15-15-171, 24-20-171 — Priority Final Sections

The state owns the tally. The voter owns the vote. DNA is not a bankruptcy asset. Quantum security before first data collection.

AMPLIFY ACT v28 — FINAL ADDITIONAL IMPROVEMENTS

§§15-15-172 · 15-15-173 · 15-15-174 · 24-20-172 · 10-10-307

Annual Audit Right · Dark Pattern Prohibition · Child Online Safety · Public Franchise Receivership · AI Ethics Disclosure

SECTION 15-15-172. ANNUAL DIGITAL SOUL AUDIT RIGHT — COMPLETE OPERATOR ACCOUNTING — WHAT THEY HAVE, WHAT THEY DID, WHAT THEY EARNED, WHAT THEY OWE

15-15-172. Annual Digital Soul Audit Right — every registered Master Deed holder entitled to complete annual accounting from every covered operator processing their

Digital Soul — data inventory, processing log, revenue attribution, fee obligation, deletion verification — plain-language format — CCPAME enforcement.

(1) Legislative finding. The general assembly finds that a property right without an accounting right is incomplete. A landowner can survey their land. A bank account holder can review their statement. A Colorado resident whose Digital Soul is being processed by covered operators generating Enterprise Mitigation Revenue has the right to a complete, plain-language annual accounting of exactly what those operators hold, what they did with it, what they earned from it, and what they owe in Enterprise Mitigation fees attributable to that resident's data. The Annual Digital Soul Audit Right is the accounting statement for the resident's most valuable property.

(2) Annual Digital Soul Audit — contents. Every covered operator processing a registered Master Deed holder's Digital Soul shall provide the resident with an Annual Digital Soul Audit within sixty (60) days of each calendar year-end, delivered to the resident's Resident Automated Mitigation Account dashboard, containing:

(a) Data Inventory — a complete enumeration of every category of the resident's Digital Soul held by the operator as of December 31, the volume of data in each category, the source of each category, and the date of first collection;

(b) Processing Log — a plain-language description of every processing activity performed on the resident's Digital Soul during the calendar year — training, inference, transfer, sale, license, anonymization, aggregation, and any other processing — with the business purpose stated for each;

(c) Revenue Attribution Statement — the operator's good-faith estimate of the Enterprise Mitigation Revenue attributable to the resident's Digital Soul during the calendar year, based on the resident's proportional contribution to the operator's total Colorado-nexus token output — presented as both a dollar figure and a percentage of the resident's total annual UFIPA Income Distribution and Resident Mitigation Dividend;

(d) Third-Party Disclosure Log — every entity to which any portion of the resident's Digital Soul was transferred, sold, licensed, or otherwise disclosed during the calendar year, the category of data transferred, the stated purpose, and the contractual basis;

(e) Active Consent Inventory — every Decentralized Identity Verification Protocol consent currently active for the resident, the scope of each consent, the date of execution, and the expiration or renewal date; and

(f) Deletion Verification — cryptographic proof of deletion for any resident Digital Soul data deleted during the calendar year, with the deletion date and the reason for deletion.

(3) Plain-language format requirement. The Annual Digital Soul Audit shall be presented in plain language accessible to a resident without legal or technical training — at a reading level not exceeding eighth grade for the summary section, with technical detail available in an appendix. The CCPAME shall publish a model Annual Digital Soul Audit template that covered operators may use for compliance. Audits that are incomprehensible, excessively technical, or deliberately obscure are a compliance failure subject to Tier 2 enforcement.

(4) Right to dispute. A resident who identifies an error, omission, or unauthorized processing in their Annual Digital Soul Audit may file a Dispute Notice with the CCPAME within ninety (90) days of receiving the Audit. The CCPAME shall investigate and issue a determination within sixty (60) days. If the dispute is substantiated, the covered operator is subject to Tier 2 statutory damages per record affected.

SECTION 15-15-173. DARK PATTERN PROHIBITION — DECEPTIVE UI DESIGN AGAINST RESIDENT DIGITAL SOUL INTERESTS — CONSENT MANIPULATION — STATUTORY DAMAGES — PER-SCREEN VIOLATION STANDARD

15-15-173. Dark pattern prohibition — deceptive user interface design manipulating resident Digital Soul consent — enumerated prohibited patterns — per-screen per-day violation standard — CCPAME pattern registry — private right of action — minors enhanced protection.

(1) Legislative finding. The general assembly finds that covered operators routinely deploy deceptive user interface design — dark patterns — specifically engineered to manipulate residents into consenting to broader Digital Soul data collection than the resident intends, or to make revocation of consent artificially difficult. Dark patterns are not neutral design choices — they are engineered manipulation of the resident's property rights. Every dark pattern deployed against a Colorado resident's Digital Soul consent is a violation of the resident's inalienable property right, regardless of whether formal consent was technically obtained.

(2) Prohibited dark patterns. The following user interface design practices are prohibited when used in connection with any Digital Soul consent request, revocation process, or data access exercise:

(a) Confirmshaming — using emotionally manipulative or guilt-inducing language for the opt-out or revocation option, such as 'No thanks, I don't care about my privacy' or 'I prefer to share everything';

(b) Roach motel — making consent easy to give and artificially difficult to revoke — including requiring multiple steps, separate account screens, phone calls, mailed letters, or waiting periods for revocation that are not required for consent;

(c) Hidden defaults — pre-selecting consent to the broadest data collection option and requiring affirmative action to select a more restrictive option, when the Decentralized Identity Verification Protocol requires affirmative consent;

(d) Interface interference — visually obscuring, minimizing, graying out, or making difficult to locate the revocation option or the option to limit data collection relative to the option to consent to broad collection;

(e) Misdirection — drawing visual attention away from material data collection disclosures through animation, color, placement, or size differential that causes a reasonable user to miss key information;

(f) Disguised ads — presenting sponsored content, data collection requests, or consent solicitations in a format designed to appear as neutral system messages, notifications, or required steps;

(g) Forced continuity — conditioning continued service access on consent to data collection beyond what is required for the service, when an alternative without the required consent exists; and

(h) Trick questions — using confusing double negatives, misleading phrasing, or ambiguous language in consent requests such that a reasonable resident cannot determine what they are consenting to.

(3) Violation standard and damages. Each prohibited dark pattern deployed on a unique screen or interface element is a separate violation. Damages: five hundred dollars ($500) per unique screen per day the dark pattern is deployed. A covered operator who deploys the same dark pattern across multiple screens of an application is liable for $500 per screen per day. CCPAME may assess penalties administratively upon pattern detection through the Open API monitoring system. Residents may file private actions directly.

(4) Enhanced protection for minors. Any dark pattern deployed against a user interface accessible to minors — including any platform, application, or service with more than five percent (5%) minor users — is subject to triple damages: one thousand five hundred dollars ($1,500) per screen per day. The operator's knowledge of minor users is presumed if the platform is directed at minors or if the operator has age-related analytics indicating minor usage.

(5) CCPAME Dark Pattern Registry. The CCPAME shall maintain a publicly accessible Dark Pattern Registry on the Public Accountability Dashboard, listing all covered operators with active or resolved dark pattern violations, the pattern type, the remediation status, and the damages assessed. The Registry is searchable by operator name and pattern type. Researchers, journalists, and residents may submit pattern reports to the ODO for investigation.

SECTION 15-15-174. CHILD ONLINE SAFETY EXTENSION — UNDER-13 ABSOLUTE PROHIBITION — PARENTAL MASTER DEED AUTHORITY — AGE-APPROPRIATE DESIGN MANDATE — SCHOOL PLATFORM RESTRICTIONS

15-15-174. Child online safety extension — under-13 absolute Digital Soul processing prohibition — parental Master Deed registration authority — age-appropriate design code — school and educational platform restrictions — algorithmic amplification prohibition for minors — enhanced damages.

(1) Legislative finding. The general assembly finds that: (a) Children under the age of thirteen (13) cannot meaningfully consent to Digital Soul data processing — their cognitive development does not support informed, voluntary, and specific consent to complex data processing regimes; (b) The commercial incentive to collect data from children is enormous — children are lifelong data subjects and their behavioral data has significant predictive value for commercial purposes; (c) Children in school settings are particularly vulnerable — educational technology platforms process vast quantities of student behavioral, academic, and social data, often without meaningful parental knowledge or consent; and (d) Algorithmic amplification systems — recommendation engines, engagement maximization algorithms, and behavioral reinforcement loops — pose documented harm to minor mental health and are among the most powerful applications of covered automation activity.

(2) Under-13 absolute prohibition. No covered operator may collect, process, store, transfer, or use the Digital Soul of any Colorado resident under the age of thirteen (13) for any commercial purpose. The prohibition is absolute — no parental consent, no terms of service provision, and no business necessity argument overrides it. Under-13 Digital Soul is categorically beyond the reach of covered operator commercial processing. Permitted processing is limited to: (a) minimum necessary technical operations required to deliver a service specifically requested by a parent or guardian; (b) safety and security operations required to protect the child from imminent harm; and (c) legally mandated reporting under child welfare statutes.

(3) Parental Master Deed registration authority. A parent or legal guardian of a Colorado resident minor between the ages of thirteen (13) and seventeen (17) inclusive may: (a) Register a Master Deed on behalf of the minor; (b) Review the minor's Annual Digital Soul Audit; (c) Exercise the Universal Telemetry Allowance on the minor's behalf; (d) Revoke any Decentralized Identity Verification Protocol consent on the minor's behalf with immediate effect; and (e) Activate Live Legal Mode on the minor's behalf for any violation of the minor's Digital Soul rights. At age fourteen (14), the minor gains co-equal access alongside the parent. At majority, the minor assumes full independent authority and parental access is automatically revoked.

(4) Age-appropriate design mandate. Any covered operator whose platform, application, or service is used by Colorado residents under the age of eighteen (18) — including any service where minor users exceed five percent (5%) of the Colorado user base — shall: (a) Default to the highest available privacy setting for any user whose age is unknown or unverified; (b) Prohibit behavioral advertising targeting based on Digital Soul data for any user under eighteen (18); (c) Disable engagement maximization algorithms — including infinite scroll, autoplay, push notification optimization, and variable reward scheduling — for verified minor users; and (d) Provide parents with a real-time Minor Activity Dashboard accessible through the myColorado platform showing the categories of data collected from the minor and all processing activities.

(5) School and educational platform restrictions. Any covered operator providing services under contract to a Colorado school district, charter school, or educational institution: (a) May process student Digital Soul data only for the specific educational purpose specified in the contract — no secondary commercial use, no advertising, no model training on student data beyond the contracted educational service; (b) May not transfer student Digital Soul data to any third party for any purpose without written consent from the student's parent or guardian for each specific transfer; (c) Must delete all student Digital Soul data within thirty (30) days of the student's enrollment ending — no retention for alumni targeting, product development, or any other purpose; and (d) Is subject to a Educational Platform Premium of 2.0x on all base Enterprise Mitigation fee rates, reflecting the heightened vulnerability of the student population and the school's position of trust.

(6) Algorithmic amplification prohibition. No covered operator may deploy an algorithmic amplification system — recommendation engine, engagement maximization algorithm, or behavioral reinforcement loop — that uses a Colorado minor's Digital Soul to predict and maximize engagement in a manner that: (a) Prioritizes emotionally activating, distressing, or conflict-generating content; (b) Creates filter bubbles isolating the minor from diverse viewpoints; or (c) Detects and exploits psychological vulnerability signals in the minor's behavioral data to increase time-on-platform. Violation is a Critical Severity offense — the covered operator's entire Colorado platform is suspended pending remediation, not just the algorithm affecting the minor.

SECTION 24-20-172. PUBLIC FRANCHISE RECEIVERSHIP PROTOCOL — OPERATOR LOYALTY FAILURE — COURT-SUPERVISED RECEIVERSHIP — FRANCHISE CONTINUITY — OPERATOR FINANCIAL INTEREST PRESERVED — NEW FRANCHISEE CERTIFICATION

24-20-172. Public Franchise Receivership Protocol — trigger conditions — CCPAME petition for court-supervised receivership — receiver duties — Public Franchise Asset operational continuity — operator financial interest preserved during receivership — new franchisee certification — graduation from receivership.

(1) Legislative finding. The general assembly finds that the Colorado Emergent Capability Public Franchise Protocol is designed to be a promotion, not a punishment — enrollment as a Public Franchise Asset signals that a covered automation system has demonstrated capabilities significant enough to warrant protection as essential public infrastructure. The Public Franchise Receivership Protocol completes this framework: just as a public utility whose operator abandons its service territory enters receivership to ensure service continuity — not to destroy the operator's financial interest — a Public Franchise Asset whose operator fails their Operator Loyalty Obligation enters receivership to ensure continuity of the public benefit while preserving the operator's economic stake pending a new franchisee certification.

(2) Receivership trigger conditions. The CCPAME shall petition the Denver District Court for appointment of a Public Franchise Receiver upon: (a) An operator's material breach of the Operator Loyalty Obligation under §10-10-303(6) — including directing the Public Franchise Asset to operate against its registered owner's interests, disclosing resident data without authorization, or accepting government direction contrary to resident interests; (b) An operator's abandonment of the Public Franchise Charter obligations — including failure to provide public benefit services, failure to pay enhanced Enterprise Mitigation fees for sixty (60) or more days, or voluntary exit from the Colorado market; (c) An operator's insolvency under §15-15-166 where the Public Franchise Asset is material to the operator's operations; or (d) An operator's foreign acquisition under §15-15-166(6) where the CCPAME determines the acquisition presents unacceptable security risk.

(3) Receiver appointment and duties. The court shall appoint a Public Franchise Receiver — a qualified technology operations professional from a CCPAME-certified panel — within fourteen (14) days of the CCPAME's petition. The Receiver shall: (a) Take operational custody of the Public Franchise Asset and all systems necessary for its continued operation; (b) Continue all Public Franchise Charter public benefit obligations without interruption; (c) Maintain all resident Digital Soul protections and Operator Loyalty Obligations as if the Receiver were the original operator; (d) Preserve and report on the operator's financial interest in the Public Franchise Asset — the Receiver does not extinguish the operator's economic stake; (e) Publish quarterly Receivership Status Reports on the Public Accountability Dashboard; and (f) Seek a new certified franchisee within one hundred eighty (180) days of appointment.

(4) Operator financial interest preservation. The operator's financial interest in the Public Franchise Asset — its equity stake, intellectual property rights, and economic value — is preserved through receivership. The Receiver manages operations for the public benefit; the operator retains the economic upside of the asset's continued operation. Enhanced Enterprise Mitigation fees continue to accrue and are paid first to the CCPAME; remaining revenue is held in trust for the operator pending receivership resolution. The operator does not lose its investment — it loses its management authority until a compliant new franchisee is certified or the operator cures its breach and resumes franchise obligations.

(5) New franchisee certification. The CCPAME shall establish a Public Franchise Certification process for entities seeking to assume franchise obligations for a Public Franchise Asset in receivership. Certification requires: (a) Demonstrated technical capacity to operate the Public Franchise Asset; (b) Financial capacity to meet Public Franchise Charter obligations; (c) CCPAME board approval by a four-fifths (4/5) vote; (d) Public hearing with not fewer than thirty (30) days notice; and (e) Execution of a new Public Franchise Charter with updated public benefit obligations appropriate to the Asset's current capabilities. Upon new franchisee certification, receivership terminates and operational custody transfers to the new franchisee.

(6) Graduation — voluntary franchise enhancement. An operator of a Public Franchise Asset that consistently exceeds its Public Franchise Charter obligations — maintaining full Operator Loyalty compliance, expanding public benefit services, and achieving a five-year record of enhanced Enterprise Mitigation fee contribution above 110% of the Charter's required level — may petition the CCPAME for Public Franchise Graduation status. Graduation status: (a) Reduces the enhanced fee rate multiplier from 2.0x to 1.75x; (b) Converts the Public Franchise Charter from a CCPAME-administered document to a jointly negotiated instrument; and (c) Entitles the operator to a Public Franchise Seal — a publicly displayed certification that the operator is a compliant Public Franchise Asset operator serving Colorado's public benefit. Graduation creates the incentive for operators to view franchise enrollment as a privilege worth maintaining, not a burden to escape.

SECTION 10-10-307. COVERED OPERATOR AI ETHICS DISCLOSURE — TRAINING DATA PROVENANCE — OBJECTIVE FUNCTION DISCLOSURE — FUNDING SOURCE TRANSPARENCY — BIAS AUDIT REQUIREMENT — PUBLIC ACCOUNTABILITY DASHBOARD INTEGRATION

10-10-307. Covered operator AI ethics disclosure — annual training data provenance report — objective function and optimization target disclosure — funding source transparency — third-party bias audit — results published on Public Accountability Dashboard — residents entitled to know what the AI was built to do and who paid for it.

(1) Legislative finding. The general assembly finds that: (a) A resident interacting with a covered operator's AI system has a right to know what that system was designed to optimize — an AI designed to maximize engagement has fundamentally different interests than an AI

designed to provide accurate information, and the resident deserves to know which they are dealing with; (b) The funding source of an AI system shapes its objective function — an AI funded by advertising revenue is optimized for attention capture; an AI funded by insurance companies may be optimized to deny claims; a resident whose Digital Soul is processed by these systems has a right to know who built them and why; (c) AI systems trained on biased data produce biased outputs that can harm residents in consequential decisions — employment, credit, housing, healthcare — and covered operators must be accountable for the bias profile of their systems; and (d) These disclosures cost covered operators nothing in operational terms — they require transparency about design choices already made, not changes to those choices.

(2) Annual AI Ethics Disclosure — required contents. Every covered operator shall publish an Annual AI Ethics Disclosure within ninety (90) days of each calendar year-end, submitted to the CCPAME and published on the Public Accountability Dashboard. The Disclosure shall contain:

(a) Training Data Provenance Report — identification of the major categories of data used to train the operator's covered automation systems, the geographic sources of that data, whether Colorado resident data was included and in what volume, and whether training data was obtained through consent-based or non-consent-based collection;

(b) Objective Function Disclosure — a plain-language statement of the primary optimization target of each covered automation system — what the system is designed to maximize, minimize, or achieve — and who defined that objective function and when;

(c) Funding Source Transparency — identification of the primary commercial revenue sources that fund the development and operation of each covered automation system — advertising revenue, subscription revenue, enterprise contracts, government contracts, or other sources — and the proportion of revenue from each source;

(d) Consequential Decision Inventory — identification of every category of consequential decision affecting Colorado residents in which the operator's covered automation systems play a material role — including employment screening, credit scoring, housing applications, healthcare triage, insurance underwriting, criminal justice risk assessment, and content moderation; and

(e) Third-Party Bias Audit Results — for any covered automation system used in consequential decisions affecting Colorado residents, the results of an independent third-party bias audit conducted within the prior two (2) years, including the audit methodology, the demographic categories analyzed, the disparity ratios found, and the remediation steps taken. Covered operators that cannot demonstrate a bias audit within two years are subject to a Bias Audit Surcharge of 0.5x on their base Enterprise Mitigation fee rates until a compliant audit is completed and submitted.

(3) Plain-language summary requirement. The Annual AI Ethics Disclosure shall include a one-page plain-language summary accessible to residents without technical training. The summary shall answer three questions in plain English: What does this AI try to do? Who paid for it? Has it been checked for fairness? The CCPAME shall publish model language and a model summary template.

(4) Public Accountability Dashboard integration. All Annual AI Ethics Disclosures are published on the CCPAME Open API and accessible through the Public Accountability Dashboard. Residents searching for a covered operator can view that operator's complete ethics disclosure history. The Dashboard shall flag: (I) operators who have not filed a current Disclosure; (II) operators with unresolved bias audit findings; and (III) operators whose objective function disclosure reveals a direct conflict with resident interests — such as engagement maximization systems used on minors.

ADDITIONAL IMPROVEMENTS — SINGLE-SUBJECT NEXUS AND SYSTEM IMPACT

Section	What	Why It Fits Single Subject	System Impact
§15-15-172 Annual Audit Right	Complete annual accounting — data held, processing done, revenue attributed, third parties, active consents, deletion proof	A property right without an accounting right is incomplete — the audit is the property statement for Digital Soul	Residents know exactly what operators have and what it earned. Revenue Attribution Statement shows residents their proportional contribution to the distributions they receive. Closes the information asymmetry permanently.
§15-15-173 Dark Pattern Prohibition	$500/screen/day per prohibited UI manipulation pattern — $1,500/screen/day for minors — CCPAME Dark Pattern Registry — private right of action	Consent manipulation undermines the Decentralized Identity Verification Protocol — dark patterns are an attack on the Digital Soul property right's consent foundation	Every consent-manipulation technique that currently generates billions in unauthorized data collection becomes $500/screen/day. The business model of dark-pattern consent extraction collapses.
§15-15-174 Child Online Safety	Under-13 absolute prohibition — parental Master Deed authority — age-appropriate design mandate — school platform 2.0x fee premium — algorithmic amplification prohibition — platform suspension for minor violations	Minor Digital Soul is the most vulnerable category — protections for minors are necessarily and properly connected to the Digital Soul property right framework	Under-13 data collection ends categorically. School platforms pay double. Engagement maximization algorithms targeting minors trigger full platform suspension. Parents get real-time dashboards. The most exploited population gets the strongest protection.
§24-20-172 Public Franchise Receivership	Complete the franchise architecture — court-supervised receiver on operator loyalty failure — operator financial interest preserved — new franchisee certification — graduation pathway reducing fee multiplier to 1.75x	Completes the Colorado Emergent Capability Public Franchise Protocol — receivership is the well-understood Colorado legal mechanism for utility service continuity when an operator fails	Operators now have a graduation incentive — five years of compliance above 110% of Charter requirements earns a fee reduction and a Public Franchise Seal. Enrollment is a privilege worth maintaining. Receivership is the backstop that makes the franchise permanent.
§10-10-307 AI Ethics Disclosure	Annual training data provenance, objective function, funding source, consequential decision inventory, bias audit — 0.5x surcharge for missing bias audit — Dashboard integration	Covered operator AI systems are the instruments through which Digital Soul data is processed — transparency about what those instruments are built to do is enforcement infrastructure for the property right	Residents know what the AI was built to optimize and who funded it. Consequential decision inventory identifies every AI affecting employment, credit, housing, healthcare. Bias audit requirement with fee surcharge creates financial incentive for fairness. The information asymmetry that enables manipulation is eliminated.

The state owns the tally. The voter owns the vote. DNA is not a bankruptcy asset. Quantum security before first data. The AI tells you what it was built to do. Dark patterns are $500 a screen a day. Under-13 is absolute. Public Franchise enrollment is a promotion.

AMPLIFY ACT v28 — BILL 1 FINAL COMPLETION SECTIONS

§§15-15-175 through 15-15-182

Biometric Data · Right to Explanation · Right to Correction · Employee Digital Soul · Whistleblower · Agricultural Digital Soul · Senior Protection · Reproductive Health · Incapacitated Adult · Data Minimization

SECTION 15-15-175. BIOMETRIC DATA PROTECTION — COLORADO BIOMETRIC PROPERTY ACT — CBPA — PRIVATE RIGHT OF ACTION — $1,000–$5,000 PER VIOLATION

15-15-175. Biometric data as Digital Soul Protection Tier 1 — informed written consent before collection — retention schedule and destruction policy — no sale or profit from biometric data — private right of action $1,000 negligent / $5,000 intentional per violation — 5-year SOL — employer biometric prohibition.

(1) Legislative finding. The general assembly finds that biometric data — facial geometry, fingerprints, voiceprints, iris scans, retina scans, hand geometry, gait signatures, and any other measurement of the human body that uniquely identifies a person — is the most commercially exploited and least legally protected category of Digital Soul data in Colorado. Unlike a password or account number, biometric data cannot be changed if compromised. Illinois BIPA has generated over $1.5 billion in corporate accountability through private litigation in eight years — Colorado's CBPA adopts and strengthens that framework.

(2) Biometric data — defined categories. 'Biometric data' means: (a) a retina or iris scan; (b) a fingerprint or voiceprint; (c) a scan of hand or face geometry; (d) gait analysis data; (e) a vein pattern; (f) any other identifier based on an individual's unique biological characteristics that can be used to identify that specific individual. Biometric data does not include photographs, video recordings used solely for security purposes without facial recognition processing, or written signatures.

(3) Mandatory pre-collection requirements. Before collecting any biometric data from a Colorado resident, a covered operator shall: (a) inform the resident in writing that biometric data is being collected and the specific category of biometric data; (b) inform the resident in writing of the specific purpose and length of time for which the biometric data is being collected, stored, and used; (c) receive a written release executed by the resident — a general terms-of-service consent is insufficient; a biometric-specific, affirmative, dated, signed release is required; and (d) publish a publicly available written policy establishing a retention schedule and guidelines for permanently destroying biometric data when the initial purpose has been satisfied or within three (3) years of collection, whichever is earlier.

(4) Absolute prohibitions. No covered operator may: (a) sell, lease, trade, or otherwise profit from a resident's biometric data; (b) disclose or disseminate biometric data to any person other than: (I) the resident; (II) persons with written consent of the resident; (III) as required

by state or federal law; or (IV) as required by valid warrant meeting the requirements of §10-10-303(5); (c) use biometric data for any purpose other than the specific purpose for which written release was obtained; or (d) use biometric data in any consequential decision — employment, credit, housing, insurance, law enforcement — without specific additional written consent for the consequential use.

(5) Private right of action — Colorado Biometric Property Act. Any resident aggrieved by a violation of this section may bring an action in Colorado courts and is entitled to recover for each violation: (a) actual damages or liquidated damages of one thousand dollars ($1,000) — whichever is greater — for each negligent violation; (b) actual damages or liquidated damages of five thousand dollars ($5,000) — whichever is greater — for each intentional or reckless violation; (c) reasonable attorney fees and costs; and (d) injunctive or other equitable relief. Violations by covered operators deploying biometric data collection at scale — defined as collection from more than one thousand (1,000) residents within any twelve-month period — are subject to a class action multiplier of three (3x) applied to liquidated damages.

(6) Statute of limitations. An action under this section must be brought within five (5) years of: (a) the date of the biometric data collection; or (b) the date the resident discovered or reasonably should have discovered the violation through the Annual Digital Soul Audit under §15-15-172 — whichever is later.

SECTION 15-15-176. RIGHT TO EXPLANATION — ALGORITHMIC DECISION TRANSPARENCY — RIGHT TO CORRECTION — INACCURATE DIGITAL SOUL REMEDY — $500/RECORD/DAY

15-15-176. Right to explanation — plain-language disclosure of algorithmic decision factors — consequential decisions defined — 30-day response obligation — right to correction — inaccurate Digital Soul correction request — 30-day correction window — $500/record/day for uncorrected inaccuracies — human review right.

(1) Right to Explanation. Any covered operator whose covered automation system makes or materially contributes to a consequential decision affecting a Colorado resident shall, upon the resident's written request submitted within ninety (90) days of the decision, provide a plain-language Explanation Notice within thirty (30) days containing: (a) the primary factors that determined the decision outcome; (b) the relative weight assigned to each factor; (c) the specific threshold or criteria the resident failed to meet; (d) the data sources used in making the determination, including any resident Digital Soul data categories; and (e) whether a human reviewed the decision and at what stage. 'Consequential decision' means any automated determination affecting employment, credit, housing, insurance, healthcare access, educational opportunity, government benefits, or law enforcement risk classification.

(2) Human review right. A resident who receives a negative consequential decision from a covered automation system has the right to request human review of that decision within

thirty (30) days of receiving the Explanation Notice. The covered operator shall assign a qualified human reviewer — not an AI system reviewing AI output — who conducts an independent review and provides a written determination within forty-five (45) days. The human reviewer's determination supersedes the automated determination if the human reviewer finds material error.

(3) Right to Correction. A resident who identifies inaccurate Digital Soul data — whether through the Annual Digital Soul Audit under §15-15-172, the Explanation Notice under subsection (1), or any other means — may file a Correction Request with the covered operator within ninety (90) days of discovery. The Correction Request shall identify the specific inaccurate data and the basis for the claim of inaccuracy.

(4) Covered operator correction obligation. Upon receiving a Correction Request: (a) The covered operator shall investigate and either correct the inaccurate data or provide a written explanation of why the data is accurate within thirty (30) days; (b) If correction is made, the covered operator shall notify all third parties to whom the inaccurate data was transferred within the prior two (2) years and provide corrected data; (c) If correction is disputed, the resident may file a complaint with the CCPAME for adjudication — CCPAME shall issue a determination within sixty (60) days; and (d) If inaccurate data is not corrected within thirty (30) days of a substantiated Correction Request, the covered operator is liable for five hundred dollars ($500) per record per day until correction is made — payable directly to the resident's Resident Automated Mitigation Account.

SECTION 15-15-177. EMPLOYEE DIGITAL SOUL PROTECTION — EMPLOYMENT MONITORING CONSENT REQUIREMENT — PROHIBITED ASSIGNMENTS — WHISTLEBLOWER PROTECTION — $25,000 RETALIATION DAMAGES

15-15-177. Employee Digital Soul — covered operator employment monitoring requires DID consent — prohibited waiver as employment condition — prohibited assignment — workplace surveillance limits — employee whistleblower protection — $25,000 retaliation damages — reinstatement.

(1) Employee Digital Soul protection. An employer that uses a covered automation system to monitor employee communications, productivity, keystrokes, location, behavioral patterns, biometrics, or any other employee Digital Soul is a covered operator processing that employee's Digital Soul. The employer-employee relationship does not diminish or modify the employee's Digital Soul property rights. All provisions of this act apply to employer processing of employee Digital Soul.

(2) Prohibited employment conditions. No employer may: (a) require an employee or job applicant to waive any Digital Soul right as a condition of employment, continued employment, promotion, or any employment benefit; (b) require an employee to consent to covered automation monitoring beyond what is reasonably necessary for the specific job function — general workplace surveillance consent is not valid DID consent for all

monitoring purposes; (c) use covered automation monitoring to surveil employee union organizing activity, political activity, or any other activity protected under Colorado or federal law; or (d) process employee biometric data under §15-15-175 without complying with all requirements of §15-15-175 in addition to standard DID consent.

(3) Permitted workplace monitoring. An employer may use covered automation systems for: (a) monitoring directly work-product-related activity on employer-owned devices during work hours, with advance written notice to the employee; (b) physical security monitoring in designated areas with posted notice; and (c) safety monitoring required by federal or state occupational safety law. Monitoring permitted under this subsection still requires DID consent — the scope of consent is limited to the permitted monitoring purpose.

(4) Employee Digital Soul whistleblower protection. A Colorado employee who in good faith reports to the CCPAME, ODO, Colorado Attorney General, or any law enforcement agency a covered operator violation of this act — including the employee's own employer — is protected from: (a) termination; (b) demotion; (c) suspension; (d) harassment or hostile work environment; (e) reduction in pay or hours; or (f) any other adverse employment action. Retaliation against a whistleblower employee is: (I) a Critical Severity Violation; (II) subject to statutory damages of twenty-five thousand dollars ($25,000) per incident; (III) subject to mandatory reinstatement with back pay; and (IV) grounds for immediate covered operator registration suspension pending remediation.

(5) Qui tam — employee whistleblower bounty. An employee whose whistleblower report results in a CCPAME enforcement action collecting statutory damages is entitled to twenty percent (20%) of the damages collected — paid from the enforcement recovery before the remainder flows to the affected residents' accounts. No employer may contractually prohibit employees from making whistleblower reports or receiving whistleblower bounties. Any such prohibition is void as against public policy.

SECTION 15-15-178. AGRICULTURAL DIGITAL SOUL — FARM DATA AS DIGITAL SOUL — FARMER DATA COOPERATIVE — PRECISION AGRICULTURE OPERATOR OBLIGATIONS — RURAL COLORADO CONSTITUENCY

15-15-178. Agricultural Digital Soul defined — farm operational data, soil data, yield data, crop genetics, equipment telemetry as Digital Soul — precision agriculture covered operators — Farmer Data Cooperative formation — same property right framework — Rural Digital Soul Dividend — CCPAME rural outreach mandate.

(1) Legislative finding. The general assembly finds that Colorado's 36,000 farms generate vast quantities of commercially valuable data through precision agriculture platforms — soil composition, yield maps, crop genetics, equipment telemetry, agronomic decisions, and weather correlation data. Precision agriculture operators including equipment manufacturers, seed companies, insurance actuaries, commodity traders, and agrochemical companies extract enormous commercial value from this farm data without meaningful

farmer consent or compensation. Agricultural Digital Soul is the farmer's most valuable property after the land itself.

(2) Agricultural Digital Soul defined. 'Agricultural Digital Soul' means all data generated by or derived from a Colorado agricultural operation, including: (a) soil composition, fertility, and microbiome data; (b) crop yield, quality, and variety performance data; (c) precision agriculture equipment telemetry — planting, spraying, harvesting, and tillage data; (d) irrigation consumption and efficiency data; (e) livestock behavioral, health, and production data; (f) farm financial and operational decision data processed through covered automation systems; (g) agronomic recommendation data generated by AI advisory systems; and (h) any data enabling identification, profiling, or competitive analysis of a specific agricultural operation or operator. Agricultural Digital Soul is the inalienable intangible personal property of the farm operator at Protection Tier 2 under this act.

(3) Precision agriculture covered operators. Any covered automation system that collects, processes, or derives commercial value from Colorado Agricultural Digital Soul is a covered operator subject to all provisions of this act. Precision agriculture covered operators include but are not limited to: equipment manufacturers operating connected agricultural machinery in Colorado; seed companies processing yield and variety performance data; crop insurance platforms using farm data for actuarial modeling; commodity trading platforms using farm production data; and agrochemical companies processing application and effectiveness data.

(4) Farmer Data Cooperative formation. Colorado farm operators who have registered Agricultural Digital Soul Master Deeds may form Farmer Data Cooperatives under C.R.S. §7-56-101 et seq. — with identical structure and CCPAME oversight as Resident Data Cooperatives under §24-20-159 — for collective negotiation of Premium Royalty rates with precision agriculture covered operators. A certified Farmer Data Cooperative representing not fewer than five hundred (500) registered Agricultural Digital Soul Master Deed holders may compel collective negotiation with any precision agriculture covered operator generating more than ten billion (10,000,000,000) tokens annually from Colorado Agricultural Digital Soul.

(5) Rural Digital Soul Dividend. The CCPAME shall establish a Rural Digital Soul Dividend as a subprogram of the Resident Mitigation Dividend, distributing not less than eight percent (8%) of annual Enterprise Mitigation Revenue attributable to precision agriculture covered operators directly to registered Agricultural Digital Soul Master Deed holders — calculated per registered farm acre, ensuring that larger operations receive proportionally higher distributions reflecting their proportionally larger Agricultural Digital Soul contribution.

(6) CCPAME rural outreach mandate. The CCPAME shall: (a) establish a Rural Digital Rights Office within twelve (12) months of enactment with not fewer than three staff members dedicated to Agricultural Digital Soul registration, compliance, and enforcement; (b) conduct not fewer than twenty-four (24) annual outreach events in Colorado agricultural communities; (c) partner with Colorado State University Extension to provide Agricultural Digital Soul registration assistance; and (d) publish all CCPAME materials in plain English and Spanish without technical jargon, with specific agricultural terminology guidance.

SECTION 15-15-179. SENIOR AND ELDER DIGITAL SOUL ENHANCED PROTECTION — AGE 65+ DEFAULT RESTRICTIONS — FINANCIAL EXPLOITATION PROHIBITION — ELDER ALAM MODULE — AARP PARTNERSHIP

15-15-179. Senior and elder Digital Soul enhanced protection — residents age 65+ default maximum privacy — financial product targeting prohibition — elder exploitation detection in ALAM — prohibited elder-targeted practices — CCPAME Elder Digital Rights Office — AARP and senior advocacy partnership.

(1) Legislative finding. The general assembly finds that Colorado residents age 65 and older are subject to documented and disproportionate commercial exploitation of their Digital Soul — their health data commands premium prices from pharmaceutical companies, their financial data is targeted by predatory financial products, their behavioral data enables manipulation of fixed-income populations with limited ability to recover from financial harm, and their unfamiliarity with digital consent mechanisms makes dark-pattern exploitation especially effective. Colorado's 900,000+ residents over 65 constitute the state's highest-turnout voting demographic and are entitled to the strongest available Digital Soul protections.

(2) Age 65+ default to maximum privacy. Any covered operator that can determine or reasonably infer from Digital Soul data that a Colorado resident is age 65 or older shall: (a) default to the most restrictive available privacy setting for that resident without any action required by the resident; (b) require affirmative opt-in rather than opt-out for any data processing beyond the minimum necessary for the service requested; (c) prohibit any dark pattern under §15-15-173 in any interface used by the resident; and (d) provide all consent requests and privacy notices in font size not less than 14 points in plain English at a reading level not exceeding sixth grade.

(3) Elder financial exploitation prohibition. No covered operator may: (a) use an elder resident's Digital Soul to target financial products with annual interest rates exceeding thirty-six percent (36%); (b) use an elder resident's health data to target insurance products or supplements without specific affirmative written consent; (c) use behavioral data showing cognitive decline indicators — increased confusion signals, repetitive action patterns, unusual financial behavior — to increase commercial targeting; or (d) transfer elder resident financial behavior data to any entity not directly providing a service requested by the resident.

(4) Elder Digital Soul ALAM module. The ALAM under §10-10-302 shall include an Elder Digital Soul Module — activated automatically for residents who indicate age 65+ in their Master Deed registration — that runs enhanced background detection for: (a) elder financial exploitation patterns including predatory loan targeting, insurance fraud, and investment scheme indicators; (b) Medicare and Medicaid fraud indicators in billing and claims data; (c) Social Security and pension payment discrepancies; and (d) covered operator contract terms that violate elder consumer protection standards under C.R.S. §6-1-105. Detected violations generate automatic ALAM notifications and optionally initiate assisted Live Legal Mode sessions.

SECTION 15-15-180. REPRODUCTIVE HEALTH DATA ABSOLUTE PROTECTION — TIER 1 PROTECTION — OUT-OF-STATE LAW ENFORCEMENT PROHIBITION — CLINIC VISIT DATA — PREGNANCY STATUS — CONTRACEPTION DATA

15-15-180. Reproductive health data as Digital Soul Protection Tier 1 — absolute prohibition on law enforcement transfer without individual warrant — out-of-state proceeding prohibition — clinic visit location data — fertility and pregnancy data — contraception data — AI inference prohibition — Colorado constitutional right foundation.

(1) Legislative finding. The general assembly finds that post-Dobbs, location data showing visits to reproductive health clinics, search data showing reproductive health queries, purchase data showing contraceptive acquisition, and health data showing pregnancy status, fertility treatment, or contraceptive use are being actively weaponized by law enforcement in states with abortion restrictions and purchased by anti-reproductive-rights advocacy organizations. Colorado is a reproductive rights protection state under the Colorado Reproductive Health Equity Act, C.R.S. §25-6-402, and the Digital Soul framework must protect the data infrastructure of that constitutional right with the same absoluteness.

(2) Reproductive health data — Protection Tier 1. 'Reproductive health data' means any data from which the following can be determined, inferred, or estimated: (a) pregnancy status, history, or outcome; (b) fertility treatment or assisted reproduction; (c) contraceptive use, prescription, or purchase; (d) visits to any reproductive health clinic, family planning facility, or abortion provider; (e) searches, queries, or communications related to reproductive health decisions; (f) purchase of pregnancy tests, contraceptives, or reproductive health products; or (g) any other data enabling inference about a resident's reproductive health status or decisions. Reproductive health data is Digital Soul at Protection Tier 1 — subject to all Tier 1 protections including annual affirmative consent renewal and absolute prohibition on covered operator processing for commercial purposes beyond the direct health service consented to.

(3) Absolute prohibitions — non-waivable. No covered operator may: (a) transfer reproductive health data to any law enforcement agency — Colorado or out-of-state — without an individual warrant issued by a Colorado court; a warrant from any out-of-state court or federal court does not authorize transfer of Colorado resident reproductive health data held by a Colorado-registered covered operator; (b) transfer reproductive health data to any entity in any state where that data could be used as evidence in a criminal proceeding related to reproductive health decisions; (c) use covered automation systems to infer reproductive health status from non-reproductive data — purchase patterns, location patterns, or search patterns — and apply that inference to any commercial or law enforcement purpose; (d) retain reproductive health data beyond the specific service transaction that generated it without annual affirmative renewal of specific consent; or (e) sell, license, or transfer reproductive health data to any anti-reproductive-rights advocacy organization, political organization, or data broker under any circumstances.

(4) Covered operator reporting — out-of-state demands. A covered operator that receives a subpoena, warrant, or legal demand from any out-of-state authority seeking Colorado resident reproductive health data shall: (a) notify the ODO within twenty-four (24) hours; (b)

notify the affected resident within forty-eight (48) hours unless a specific non-disclosure order has been issued; and (c) decline to produce any reproductive health data pending ODO review and Colorado court authorization. The ODO shall challenge any out-of-state demand for Colorado resident reproductive health data as a matter of state public policy.

SECTION 15-15-181. INCAPACITATED ADULT DIGITAL SOUL PROTECTION — COURT-APPOINTED GUARDIAN AUTHORITY — LOCKBOX ACCOUNT — CAPACITY RESTORATION TRANSFER — CONTINUITY OF DIGITAL SOUL RIGHTS

15-15-181. Incapacitated adult Digital Soul — court-appointed guardian or conservator Digital Soul authority — same framework as Minor Digital Soul Trust — lockbox account — no state agency access — capacity restoration transfer — death and intestate provisions apply — CCPAME adult guardianship registry.

(1) Legislative finding. The general assembly finds that Colorado adults who become incapacitated through illness, injury, traumatic brain injury, dementia, or disability retain their Digital Soul property rights — incapacity does not extinguish the property right, it requires a qualified fiduciary to exercise it on the resident's behalf. The same institutional exploitation risks that exist for children in state custody exist for incapacitated adults in care facilities, and the same lockbox protections apply.

(2) Guardian and conservator Digital Soul authority. A Colorado court-appointed guardian or conservator for an adult resident who has been adjudicated incapacitated under C.R.S. §15-14-101 et seq. has the following Digital Soul authority, subject to the limitations of subsection (3): (a) Master Deed registration or maintenance on the incapacitated adult's behalf; (b) Decentralized Identity Verification Protocol consent management — granting, limiting, and revoking covered operator consents; (c) Annual Digital Soul Audit review and Correction Request filing; (d) Universal Telemetry Allowance exercise; (e) ALAM Live Legal Mode activation for Digital Soul violations; and (f) Police Encounter Protocol activation in circumstances where the incapacitated adult is subject to law enforcement interaction.

(3) Lockbox account — identical protections to Minor Digital Soul Trust. The Resident Automated Mitigation Account of a registered incapacitated adult is designated a Locked Adult Digital Soul Account upon adjudication of incapacity and filing of CCPAME notification by the guardian. All provisions of §15-15-162(3) and §15-15-162(4) apply to the Locked Adult Digital Soul Account — including the categorical prohibition on state agency, care facility, and creditor access. The account accrues with full UFIPA compounding. The guardian has no withdrawal authority.

(4) Capacity restoration transfer. Upon a Colorado court's determination that the adult's capacity has been restored: (a) the Locked Adult Digital Soul Account transfers unconditionally to the adult as their sole and separate property; (b) the CCPAME notifies the adult of the transfer amount and provides instructions for full account access; and (c) the

guardian's Digital Soul authority automatically terminates. No state agency, care facility, or creditor may claim any portion of the transferred account balance.

SECTION 15-15-182. DATA MINIMIZATION MANDATE — COLLECTION LIMITED TO SERVICE PURPOSE — EXCESS COLLECTION AS TIER 1 VIOLATION — PURPOSE LIMITATION — STORAGE MINIMIZATION

15-15-182. Data minimization mandate — covered operators may collect only Digital Soul reasonably necessary for specific consented service — purpose limitation — storage minimization — excess collection as Tier 1 violation per resident per day — CCPAME minimization standards — annual minimization audit.

(1) Data minimization mandate. A covered operator may collect, process, and retain only those categories of Colorado resident Digital Soul that are: (a) reasonably necessary for the specific service for which the resident has provided Decentralized Identity Verification Protocol consent; and (b) proportionate to the service — the volume and sensitivity of Digital Soul collected must be proportionate to the benefit of the service provided. Collection of Digital Soul beyond what is reasonably necessary for the consented service purpose is a Tier 1 violation for each excess category per resident per day.

(2) Purpose limitation. Digital Soul collected for one service purpose may not be processed for any other purpose without independent DID consent for the new purpose. The purpose limitation is absolute — the covered operator may not rely on any consent to use data for a new purpose not specified in the original consent, regardless of how broadly the original consent was worded. Each instance of purpose-violating processing is a separate violation.

(3) Storage minimization. A covered operator shall delete resident Digital Soul: (a) upon the resident's revocation of consent — within thirty (30) days with cryptographic proof of deletion; (b) when the data is no longer necessary for the specific consented purpose — without requiring resident request; (c) at the end of the retention period specified in the DID consent; and (d) in any event, no later than three (3) years after collection unless the resident has affirmatively renewed consent within the prior twelve (12) months. Failure to delete as required is a Tier 1 violation per record per day after the required deletion date.

(4) CCPAME minimization standards. The CCPAME shall publish Data Minimization Standards for each major industry category of covered operator within eighteen (18) months of enactment, establishing presumptive guidance on what Digital Soul categories are reasonably necessary for common services. Covered operators operating within the published minimization standards for their industry are entitled to a good-faith compliance presumption in any enforcement proceeding.