STATE OF WYOMING

Select Committee on Blockchain, Financial Technology and Digital Innovation Technology

WYOMING PERSONAL DATA OWNERSHIP ACT

Draft Version Alt-21.7 — Consolidated Structure

Title 34, Chapter 31 — W.S. 34-31-101 through 34-31-109

AN ACT relating to property; establishing personal data as the intangible personal property of natural persons; providing for the rights of data owners, the classification and protection of personal data, access authority, the duties of data custodians, enforcement, federal law accommodation, and administration; providing definitions; making a conforming amendment; and providing for effective dates.

This consolidated draft preserves the full substance of Draft Version 21 in eight operative sections. It expresses each governing principle once and relies on defined terms, a unified access-authority framework, a functional sensitive-data standard, and consolidated construction rules in place of repeated enumeration. No protection, right, duty, or remedy of Version 21 is omitted. Technical specification is delegated to rules of the enforcing authority as expressly provided.

Draft for committee review. Subject to Legislative Service Office technical revision before introduction.

Be It Enacted by the Legislature of the State of Wyoming:

34-31-101. Short title; declaration; rules of construction.

(a) This chapter shall be known and may be cited as the “Wyoming Personal Data Ownership Act.”

(b) Declaration and rules of construction. The following govern the interpretation and application of this chapter:

(i) This chapter recognizes and protects a property right of Wyoming residents in their personal data, the incidents of ownership of which are defined by this chapter. Those incidents shall be construed as the legal mechanism by which the privacy, autonomy, dignity, and continuing individual control of Wyoming residents are protected, and no provision of this chapter shall be construed to authorize the permanent commercial alienation of those interests or of any incident of ownership designated non-waivable by this chapter.

(ii) A right or incident of ownership designated non-waivable by this chapter remains non-waivable notwithstanding any contract, consent, waiver, license, terms of service, employment agreement, or similar private arrangement, consistent with the arbitration rule of W.S. 34-31-107(e).

(c) This chapter shall be construed broadly in favor of the data ownership rights of Wyoming residents. Claimed lawful uses, defenses, and exceptions shall be construed narrowly and not extended by analogy. Where interpretations differ, the interpretation favoring the least use of identifiable personal data and the greatest preservation of privacy, autonomy, dignity, bodily integrity, and individual control governs. The enumeration of specific instances, examples, or categories does not exclude unenumerated instances of the same class, and “including” denotes a nonexclusive illustration.

(d) The substance and practical effect of a processing activity control over its form, label, structure, or characterization. No person may evade this chapter through contractual characterization, technological design, corporate structure, intermediary or affiliate arrangements, service-provider designation, data trust, algorithmic transformation, artificial fragmentation of processing, or any similar mechanism. Storage or retention of data in a form that preserves a practical capability for future re-identification of individuals, or for biometric extraction, constitutes possession of personal data.

(e) The rights and remedies of this chapter are minimum protections, cumulative with every constitutional, statutory, common-law, and equitable right otherwise available, and supplement any right of privacy. Nothing in this chapter regulates, restricts, or imposes liability for communication, reporting, commentary, criticism, scholarship, indexing, research, or other expressive activity protected by the First Amendment or Article 1, Section 20 of the Wyoming Constitution, nor authorizes acquisition of personal data through lesser legal process than the Wyoming or United States Constitution, federal law, or Wyoming common law would otherwise require. A data license does not authorize governmental acquisition of personal data.

(f) A violation of this chapter is not a violation of the Wyoming Consumer Protection Act, W.S. 40-12-101 through 40-12-114, unless the same conduct independently constitutes a deceptive trade practice. This chapter complements the Wyoming Digital Assets Act, W.S. 34-29-101 through 34-29-106, under which personal data is not a digital asset; the Data Privacy-Government Entities Act, W.S. 9-21-201 through 9-21-203; where both address the same subject, both apply and the more protective provision governs; and the data breach notification statute, W.S. 40-12-501 through 40-12-509. Nothing in this chapter restricts access to information required to be public under the Wyoming Public Records Act, W.S. 16-4-201 through 16-4-205. The common law torts of conversion, trespass to chattels, unjust enrichment, and breach of bailment duty apply to personal data as intangible personal property.

(g) Statutes enacted after the effective date of this chapter that regulate privacy, biometric information, artificial intelligence, employment, surveillance, advertising, children's data, or related subjects supplement this chapter and do not diminish its ownership rights or non-waivable incidents absent clear and express legislative statement. Repeal, limitation, or modification by implication is disfavored. This chapter is a law of general and uniform operation consistent with Article 1, Section 34 of the Wyoming Constitution.

(h) The enforcing authority is the attorney general, who may promulgate rules under the Wyoming Administrative Procedure Act, W.S. 16-3-101 through 16-3-115, establishing technical standards for verifiable deletion and machine unlearning, procedures for exercising rights, standards for access authority and deidentification, the data broker registry and centralized deletion mechanism, minor age verification, and other matters necessary to implement this chapter. Rules shall not diminish any right or obligation established by this chapter. Not later than nine (9) months after enactment the enforcing authority shall publish plain-language compliance guidance; a data custodian acting in good-faith reliance on published guidance is not subject to statutory damages for a resulting violation it promptly corrects.

34-31-102. Definitions.

(a) As used in this chapter:

(i) "Access authority" means a data license, an owner-granted authorization, or a lawful use, each granted for a specified purpose.

(ii) "Authorized representative" means a parent or legal guardian of a minor data owner, the personal representative of a deceased data owner's estate, the holder of a power of attorney expressly authorizing exercise of rights under this chapter, or a court-appointed guardian or conservator.

(iii) "Commercial exploitation" means processing personal data primarily for monetary gain, behavioral advertising, profiling, targeted marketing, sale, licensing, monetization, commercial model development or training, enhancement of products or services offered for consideration, or any substantially similar commercial purpose. Communication within an ongoing voluntary relationship the data owner initiated and may terminate, including solicitation of voluntary contributions, and the creation, production, distribution, or promotion of an expressive work, are not commercial exploitation, provided the data is not sold, transferred, or combined with data from another source to develop individualized profiles; the use of a data owner's identity, voice, or likeness to advertise an unrelated product or service, or in merchandise distinct from the expressive work, is commercial exploitation.

(iv) "Dark pattern" means a user interface or choice architecture with the purpose or effect of impairing a data owner's ability to make a free and informed decision regarding processing of personal data.

(v) "Data broker" means a data custodian whose business, or a substantial part of it, consists of collecting, aggregating, selling, licensing, or otherwise providing access to personal data of persons with whom it has no direct relationship established for a purpose other than data collection.

(vi) "Data custodian" means any person that collects, receives, stores, processes, uses, discloses, transfers, or derives commercial value from personal data of a Wyoming resident, regardless of location or of any direct relationship with the data owner. A provider of passive technical infrastructure that does not determine the purpose or means of processing is not a data custodian solely by reason of providing that infrastructure. A service provider is not a separate data custodian unless it processes beyond the contracted service.

(vii) "Data license" means a written authorization granted by a data owner permitting processing of specified personal data for specified commercial or transactional purposes, meeting the requirements of W.S. 34-31-105(a).

(viii) “Data owner” means the natural person who is the Wyoming resident to whom personal data relates. Only a natural person may be a data owner.

(ix) “Deidentified data” means data from which re-identification of a specific individual is not reasonably feasible under the standard of W.S. 34-31-106(c).

(x) “Derived data” means data created by any computational, statistical, or inferential process applied to personal data, including predictions, scores, classifications, profiles, and inferences. Derived data reasonably linkable to an identified or identifiable natural person is “individualized derived data.” A generalized model, model weights, or aggregate system not reasonably linkable to any identified or identifiable natural person is not derived data. The inability to reconstruct the original data does not defeat linkability of embeddings, latent representations, or transformed outputs.

(xi) “Lawful use” means a statutory, non-possessory privilege to process personal data for a specific purpose under W.S. 34-31-106 without a data license or owner-granted authorization.

(xii) “Minimum necessary” means the least amount and least identifying form of personal data sufficient to accomplish the specific purpose, after application of the necessity hierarchy of W.S. 34-31-106(a).

(xiii) “Minor” means a natural person under eighteen (18) years.

(xiv) “Owner-granted authorization” means a written, voluntary permission by a data owner or authorized representative for a specific non-commercial use by an identified recipient, creating no interest described in paragraph (i) of this subsection, non-assignable, terminating on completion of the purpose, and authorizing no commercial exploitation, behavioral profiling, sale, or transfer. It is not a data license. Any arrangement so characterized that involves compensation, assignment, profiling, or commercial exploitation operates as a data license by operation of subsection (d) of W.S. 34-31-101.

(xv) “Personal data” means information linked or reasonably linkable to an identified or identifiable Wyoming resident or to a personal digital identity as defined in W.S. 8-1-102(a)(xviii). Information is reasonably linkable if it enables identification, prediction, profiling, classification, scoring, targeting, attribution, representation, or simulation of an identified or identifiable natural person; aggregation, transformation, or inference does not eliminate linkability, and derivation alone does not create it. “Personal data” does not include deidentified data, published personal expression processed consistent with W.S. 34-31-103(e), or a derived claim communicated through a zero-knowledge proof that discloses no underlying personal data beyond the claim and includes no identifier enabling attribution to a specific natural person.

(xvi) “Processing” means any operation on personal data, including collection, storage, use, disclosure, transmission, combination, training of an artificial intelligence or automated system, erasure, and destruction. It excludes transient technical operations under W.S. 34-31-106 and user-directed disclosures.

(xvii) “Published personal expression” means personal data consisting of content the data owner deliberately published for public consumption, which retains property protection against commercial exploitation of the data owner’s identity. Processing of published personal expression that does not target the data owner’s identity, produce outputs attributable to or impersonating the data owner, or derive a profile linked to the data owner is not subject to the licensing requirements of this chapter.

(xviii) “Right of reversion” means the automatic termination, upon expiration or revocation of a data license, termination of an owner-granted authorization, or completion or termination of a lawful use, of all outstanding processing authority and the resumption of the data owner’s unencumbered property rights. Title remains continuously vested in the data owner; it is the outstanding processing authority that terminates. On operation of the right of reversion the data custodian shall cease processing and, except where a statutory servitude under W.S. 34-31-108 requires retention, complete verifiable deletion within thirty (30) days and confirm deletion in writing within thirty-five (35) days.

(xix) “Sensitive data” means the categories in W.S. 34-31-104(b).

(xx) “Service provider” means a person that processes personal data on behalf of and under the instruction of a data custodian under a written agreement, solely to provide a contracted service.

(xxi) “Statutory servitude” means the limited, non-possessory right to process personal data arising by operation of law as provided in W.S. 34-31-108.

(xxii) “Transfer” means any disclosure, assignment, or sharing of personal data to a third party but does not include a disclosure to a service provider or a user-directed disclosure.

(xxiii) “User-directed disclosure” means a specific sharing of personal data initiated and controlled by the data owner in real time and is an exercise of the data owner’s property right, not a data license.

(xxiv) “Verifiable deletion” means permanent removal and destruction of personal data and individualized derived data, including copies and backups, such that it cannot reasonably be recovered, to the standard set by rule.

(xxv) “Wyoming resident” means a natural person domiciled in Wyoming. A person’s status as a Wyoming resident is determined at the time the person’s rights under this chapter are asserted, and personal data of a Wyoming resident is protected under this chapter regardless of where the person was located when the data was collected.

(xxvi) “Zero-knowledge proof” means a cryptographic protocol that proves a claim is true without conveying any information beyond the truth of the claim.

34-31-103. Personal data as intangible personal property.

(a) Personal data of a natural person is the intangible personal property of that person. Title vests in that person and remains continuously vested except through inheritance or succession. Title survives disclosure, publication, lawful access, copying, possession by another, public availability, transmission, and processing; no act that moves, copies, or makes personal data available to another affects title or any incident of ownership. Personal data is a sui generis class of intangible personal property distinct from digital assets, general intangibles, investment property, and money under title 34.1, Wyoming statutes, is not subject to article 9 of the Uniform Commercial Code, and is not abandoned or unclaimed property. On the data owner’s death, ownership passes to the estate by will or intestate succession, except that rights under this chapter with respect to a deceased data owner’s personal data may be exercised only by the authorized representative or successor in interest and terminate fifty (50) years after death.

(b) The property right is enforceable against any person that collects, processes, retains, transfers, or derives commercial value from personal data of a Wyoming resident, regardless of where processing occurs and regardless of a contractual choice of other law. The ownership interest is located in Wyoming when held by a Wyoming resident, and interference with it is an injury occurring in Wyoming.

(c) Unauthorized processing or possession of personal data is an interference with the data owner’s exclusive rights and a concrete and particularized injury that bears a close relationship to the harms traditionally redressed by the common-law actions of trespass and conversion, actionable as statutory trespass to or conversion of the data owner’s property under W.S. 34-31-107 without proof of physical or economic harm separate from the interference.

(d) Individualized derived data is an accession owned by the data owner of the underlying personal data; a data custodian may not retain, use, transfer, or derive value from it after the right of reversion operates or a deletion demand is made, and one who does is liable for conversion. Synthetic data that mirrors a data owner’s characteristics at an individual level is subject to this chapter.

(e) The public availability of personal data does not diminish ownership, and aggregation or resale of publicly available personal data is commercial processing subject to this chapter. Ownership does not include the right to prevent communication, reporting, commentary, criticism, analysis, scholarship, indexing, discovery, preservation, or the creation or distribution of an expressive work concerning the data owner, provided the processing does not create individualized derived data and does not constitute commercial exploitation of individualized information concerning the data owner. The incidental depiction of a natural person in an expressive work does not by itself create individualized derived data, constitute commercial exploitation, or require access authority. Information not reasonably linkable to an identified or identifiable natural person is not personal data and title vests in no data owner.

(f) No data custodian shall condition a product or service on a data license broader than necessary to provide it, deny an essential product or service for declining a license, or penalize the exercise of any right under this chapter; a license so obtained is void. A data custodian may offer enhanced features or reduced pricing for a voluntarily granted license if the essential product or service remains available to those who decline.

(g) Neither an access authority nor a statutory servitude conveys title to personal data or creates any ownership, possessory, equitable, contractual, transferable, or continuing interest in the holder. Neither authorizes processing beyond the specific purpose for which it was granted or arose.

34-31-104. Classification; sensitive data; rights of data owners.

(a) Ownership is uniform across all personal data. Tier classification governs licensing limits, transfer rules, legal process, and remedies; it does not affect the nature or quality of the ownership right. Personal data within more than one classification is subject to the most protective applicable classification.

(b) The following categories of personal data are sensitive data:

(i) biometric identifiers, meaning data extracted from a biological or behavioral characteristic that is used or reasonably capable of being used to identify a person, including fingerprint, retina or iris, voiceprint, facial-geometry, and gait-pattern templates;

(ii) genetic data;

(iii) neural data;

(iv) personal health data, regardless of coverage by the Health Insurance Portability and Accountability Act;

(v) precise geolocation within one thousand seven hundred fifty (1,750) feet;

(vi) religious belief data;

(vii) political affiliation data;

(viii) financial account data;

(ix) personal data of a minor; and

(x) personal data revealing or reasonably linkable to a person’s status, beliefs, associations, lawful activities, or ownership of lawful property, or presence at or association with any facility, service, organization, or gathering, where unauthorized disclosure would create a substantial risk of physical harm, harassment, intimidation, persecution, discrimination, deprivation of liberty or legal rights, or targeting of the person or the person’s lawful property, judged objectively in light of historical patterns of harm. Disclosure exposing a person to differential treatment in employment, housing, insurance, lending, or public accommodation is a substantial risk of discrimination. This category shall be construed to effectuate its protective purpose. For purposes of this paragraph, where the risk described in this paragraph is present, that risk arises upon the compilation, aggregation, or commercial availability of the data and not only upon a subsequent use or disclosure, and a data owner is not required to demonstrate that misuse has occurred.

A photograph, video, or audio recording is not itself a biometric identifier; an extracted template is sensitive from the moment of extraction and the recording remains at its otherwise applicable tier.

(c) Personal data is classified in four (4) tiers:

(i) Tier 1 is genetic data, neural data, and personal data of a minor under thirteen (13) years. It is absolutely inalienable from commercial licensing, no data license may be granted for it, any purported commercial instrument or waiver is void, and it may be processed only under a lawful use or an owner-granted authorization that involves no sale, transfer, or commercial monetization of the Tier 1 data itself. Legal process requires a warrant on probable cause.

(ii) Tier 2 is biometric identifiers, precise geolocation, and the risk-based category of subsection (b) of this section. It requires affirmative opt-in consent specific to the category, a maximum license term of twelve (12) months, a separate direct license from the data owner for any third-party transfer, and allows no cure period. Legal process requires a warrant on probable cause.

(iii) Tier 3 is personal health data, religious belief data, political affiliation data, financial account data, and personal data of a minor aged thirteen (13) through seventeen (17). It requires affirmative opt-in consent specific to the category, a maximum license term of twelve (12) months, a separate direct license for any third-party transfer, and allows no cure period. Legal process requires a court order on judicial review.

(iv) Tier 4 is all other personal data, with a maximum license term of twenty-four (24) months, retention not to exceed three (3) years from collection absent a statutory servitude, and legal process by valid subpoena.

No qualitative distinction within a tier shall be made. A statutory servitude operates on Tier 2 or Tier 3 data only to the extent and duration provided in W.S. 34-31-108, with all tier protections applying beyond that scope.

(d) Every data owner has the following rights against any data custodian, regardless of any direct relationship and exercisable through an authorized representative:

(i) to assert title to personal data as intangible personal property under W.S. 34-31-103;

(ii) to obtain within thirty (30) days a copy of personal data held, its categories, purposes, and transferees;

(iii) to correct or object under subsection (e) of this section;

(iv) to demand verifiable deletion under subsection (f) of this section;

(v) to data portability in a structured, machine-readable format within thirty (30) days;

(vi) to revoke any data license at any time without penalty;

(vii) to a description of and deletion of individualized derived data;

(viii) to make user-directed disclosures; and

(ix) to bring an action under W.S. 34-31-107.

The rights of revocation, deletion, access, reversion, and private action, and the inalienability of Tier 1 data, are non-waivable incidents of ownership under W.S. 34-31-101(b)(ii).

(e) A data owner may object in writing to the accuracy, completeness, pertinence, retention, or dissemination of personal data. Within sixty (60) days the data custodian shall verify identity, investigate, and correct, restrict, or delete the data if the objection is meritorious, or notify the data owner in writing and allow a statement of the data owner’s position to be maintained with the data, if the objection is not meritorious.

(f) A data owner may demand verifiable deletion at any time. The data custodian shall comply within thirty (30) days. Where continued retention is permitted by an active access authority or a statutory servitude, the data custodian shall state the specific basis in writing within thirty (30) days of the demand.

34-31-105. Access authority; duties of a data custodian.

(a) Personal data may be processed only under a valid access authority. A data license is valid only if it:

(i) is in writing and separate from general terms;

(ii) identifies the specific categories, purposes, and authorized processors;

(iii) states the duration within the applicable maximum and a no-penalty revocation right and mechanism;

(iv) is free of dark patterns;

(v) is not conditioned on a product or service in violation of W.S. 34-31-103(f); and

(vi) for Tier 2 or Tier 3 data, is obtained by unbundled affirmative opt-in consent specific to the category.

Consent must be freely given, specific, informed, unambiguous, and revocable; silence, pre-checked boxes, default settings, non-negotiable terms, continued use, and dark patterns are not consent. A license not meeting these requirements is void, and no license may authorize transfer to unidentified parties except service providers, perpetual or irrevocable or assignable terms, waiver of any right, or limitation of the action under W.S. 34-31-107. The data custodian bears the burden of proving a valid license. Automatic renewal is void and renewal requires a new affirmative act of consent.

(b) A data owner may revoke a data license at any time without cause or penalty through a mechanism no more burdensome than granting it, whereupon the right of reversion operates. Revocation operates prospectively: the data custodian shall cease all new and continuing processing of the personal data and shall not initiate any new reproduction or distribution of it. Revocation does not require the recall, alteration, or destruction of an expressive work that was created and published before revocation, whether or not the work remains within the data custodian’s control, but the data custodian shall not use the personal data to create a new expressive work or a new commercial use after revocation. No processing of the personal data after revocation is authorized except completion of a transaction the data owner had already requested.

(c) A data custodian holding personal data is a bailee under a digital bailment in which title remains in the data owner and owes the data owner the following duties:

(i) to maintain reasonable safeguards;

(ii) to process only for the authorized purpose and scope;

(iii) to collect and retain only the minimum necessary;

(iv) to ensure accuracy and investigate objections;

(v) to answer access requests truthfully within thirty (30) days;

(vi) to ensure service providers and recipients comply; and

(vii) to disclose on request the categories, purposes, and a reasonable estimate of revenue derived.

Processing outside any valid access authority constitutes trespass to or conversion of the data owner’s property; for Tier 2 data conversion attaches regardless of knowledge or intent, and for Tier 1 data strict liability attaches to any commercial processing beyond a lawful use or owner-granted authorization. A data custodian remains liable for its service providers except where the violation arose solely from the provider’s conduct beyond the agreement, the data custodian had no reasonable ability to prevent it, and affected data owners were notified within thirty (30) days. Service-provider obligations are enforceable by the data owner as a third-party beneficiary.

(d) No data custodian shall possess personal data without an active access authority or transfer it to a third party except under a direct license from the data owner to the recipient, to a compliant service provider, or as a lawful use; an owner-granted authorization authorizes no third-party transfer. Unauthorized possession is trespass under W.S. 34-31-103(c); storage and retention are possession. Verifiable deletion requires removal from all systems, backups, and caches, direction to service providers and recipients, commercially reasonable removal or minimization using best available technology of the data owner’s personal data and individualized derived data from any model or system that processed it with documentation of method, expected effect, and residual risk, and an auditable record; a data custodian providing false or materially incomplete attestation of verifiable deletion is liable as if no cure occurred.

(e) On a merger, acquisition, sale of assets, bankruptcy, or reorganization, all data licenses and owner-granted authorizations terminate automatically upon consummation, and a successor shall not process without new access authority. Notice shall be given to data owners not fewer than thirty (30) days before or, where prior notice is barred by applicable legal confidentiality obligations, not later than fourteen (14) days after consummation. The personal data of Wyoming residents is not an asset of the data custodian available for sale or transfer to satisfy creditor claims. Notwithstanding termination, a license for an ongoing service the data owner is actively receiving survives if the successor continues the identical service on materially identical terms, gives the required notice including the right to revoke and demand deletion, and uses the data for no new purpose; it terminates on material change or revocation. One-time transaction records do not constitute an ongoing service.

(f) The execution of an employment contract creates an employment data lease, a limited license to process employee personal data strictly necessary for administration of the employment relationship, including payroll, legal compliance, benefits, and evaluation of defined job duties, and terminating upon termination of employment, whereupon the right of reversion operates. An employer is a data custodian, may not process employee data for commercial purposes beyond administration, sell or transfer it, or retain it beyond employment except as a statutory servitude requires, and may not monitor beyond that scope; on an employee-owned device only employer-provided applications and data within that scope may be monitored.

(g) An owner-granted authorization is valid if written; identifying the recipient, specific data, and purpose; voluntary and free of dark patterns; creating no interest described in W.S. 34-31-102(a)(i); non-assignable; terminating on completion; and authorizing no commercial exploitation, profiling, sale, or transfer. It does not exempt the recipient from the bailee duties of this section. It is available for Tier 1 data, but not for any purpose involving compensation, sale, transfer, or commercial monetization of the Tier 1 data itself; for a data owner under thirteen (13) an authorized representative may grant one for Tier 1 data only for a health or welfare purpose of the data owner or the data owner’s disease community consistent with an institutional review board determination. No owner-granted authorization waives the ongoing right to deletion or to a private action.

34-31-106. Lawful uses.

(a) A lawful use authorizes processing without a data license or owner-granted authorization for the specific purpose stated, is a non-possessory privilege created and governed solely by this chapter to which no common law of easement applies, and terminates on completion of the purpose, whereupon the right of reversion operates. Lawful uses are affirmative defenses on which the data custodian bears the burden, established by a preponderance of the evidence and contemporaneous business records, of showing that the processing fell within the precise purpose, used the minimum necessary data, and did not continue after the purpose ended. A data custodian must show the purpose cannot reasonably be achieved with deidentified data and, where deidentified data is insufficient, that it cannot be achieved with less identifying data. Where deidentified data suffices, identifiable data may not be used. No lawful use authorizes commercial exploitation, sale or transfer to a data broker, behavioral advertising or profiling, retention beyond the purpose, or commercial processing of Tier 1 data. Where multiple lawful uses apply, each requirement must be satisfied and the more protective requirement governs. A lawful use invoked only to continue possession, without an independent purpose, is not valid.

(b) The following are lawful uses, each limited to the minimum necessary for its stated purpose:

(i) operational necessity, meaning processing strictly necessary to complete a transaction or provide a product or service the data owner affirmatively requested, including a continuously operating feature enabled by the data owner and that the data owner may disable at any time, with deletion within ninety (90) days of completion unless a statutory servitude requires longer or, for fraud detection, anti-money-laundering, sanctions screening, or substantially similar financial integrity functions, retention not exceeding twenty-four (24) months processed only for that documented purpose;

(ii) personal or household use with no commercial dimension, including making personal content available through a platform acting as a conduit for the person’s own expression;

(iii) bona fide journalism, investigative reporting, or public-interest accountability concerning matters of public concern, which is a single invocation;

(iv) academic or scientific research approved by an institutional review board that has determined deidentified data is insufficient, a participant’s board-approved written consent meeting the substance of W.S. 34-31-105(a) constituting an owner-granted authorization including for Tier 1 data, with reproducibility retention up to ten (10) years where a recognized authority requires it;

(v) disclosure to government only on the legal process required by W.S. 34-31-104(c), with notice to the data owner not fewer than five (5) business days before disclosure unless a court prohibits it and with judicial authority to limit, condition, or deny;

(vi) response to an imminent, specific, articulable threat to life or physical safety, limited to responders and to the emergency’s duration;

(vii) processing by a licensed professional under an independent duty of confidentiality for the specific professional service;

(viii) processing of voter registration data and voluntarily provided contact information for voter registration, education, petitioning, civic engagement, or communication concerning elections, candidates, ballot measures, or political, civic, or public affairs, construed broadly, with no sale, no profiling combination, and deletion within sixty (60) days after the election cycle except retained voluntary contact information;

(ix) professional communication using a person’s business contact information provided or published for that purpose, with no sale, profiling, or behavioral advertising and cessation on the data owner’s direction;

(x) access by a general-purpose search engine or information index to publicly available personal data for indexing where it does not commercially exploit, aggregate into personal profiles, or make secondary commercial use. Incidental commercial benefit from general indexing is not commercial exploitation, and the deletion right applies to indexed data with written basis for any denial within thirty (30) days. A person who voluntarily assumed a prominent public role may not use the deletion right to suppress indexed information about that role or conduct bearing on fitness for it.

Transient packet routing, signal maintenance, domain resolution, standard security monitoring, and transient caching do not constitute processing for purposes of this chapter where no behavioral profile is created, data is not retained beyond the duration necessary for the technical function, and there is no commercial use.

(c) Data is deidentified for purposes of this chapter where re-identification is not reasonably feasible considering all information and techniques reasonably available to a sophisticated adversary; removal of direct identifiers alone is insufficient. A qualified independent expert's written determination creates a rebuttable presumption of deidentification, and a data custodian maintaining that determination, ongoing safeguards, and contractual re-identification prohibitions on recipients bears no liability for so deidentified data. Re-identification subjects the actor to this chapter as though the data had never been deidentified, and a third party that re-identifies is independently a data custodian; the original data custodian is liable where deidentification failed the standard at transfer or it required no contractual prohibition, with apportionment otherwise.

34-31-107. Enforcement and remedies.

(a) A data owner whose rights are violated may sue in district court without proof of actual damages beyond the violation and may recover:

(i) statutory damages by tier and culpability, as follows:

(A) Tier 1, five thousand dollars ($5,000.00) per negligent violation and fifteen thousand dollars ($15,000.00) per intentional or reckless violation;

(B) Tier 2, three thousand dollars ($3,000.00) per negligent violation and ten thousand dollars ($10,000.00) per intentional or reckless violation;

(C) Tier 3, one thousand dollars ($1,000.00) per negligent violation and five thousand dollars ($5,000.00) per intentional or reckless violation; and

(D) Tier 4, five hundred dollars ($500.00) per negligent violation and two thousand five hundred dollars ($2,500.00) per intentional or reckless violation;

(ii) actual damages if greater than the applicable statutory damages;

(iii) disgorgement of unjust enrichment, measured by:

(A) the actual gain;

(B) the fair license value; or

(C) the applicable statutory damages, with doubts resolved for the data owner;

(iv) injunctive relief, including verifiable deletion; and

(v) reasonable attorney's fees and costs on prevailing.

Purely procedural or notice violations yield actual damages, injunctive relief, and fees but not statutory damages. An action for trespass to or conversion of personal data under this chapter is a statutory action whose elements are interference with the rights established by this chapter, and common-law limitations on the subject matter of conversion or trespass do not apply.

(b) All violations of the same type by the same data custodian against the same data owner arising from a single course of conduct are one (1) violation; continuation after written notice is a new violation for each thirty (30) day period. Actions may proceed as class actions under the Wyoming Rules of Civil Procedure, a common violation of a defined class of data owners establishes sufficient commonality for class certification, with aggregate disgorgement by the same measure. No action may be brought after four (4) years from discovery and in no event after ten (10) years from the violation, except that the ten (10) year limitation does not apply where the data custodian actively concealed the violation.

(c) Before suit for a Tier 4-only violation, a data owner shall give thirty (30) days written notice, and a complete cure bars the action; no cure period applies to Tier 1, Tier 2, or Tier 3 data, intentional or reckless violations, or systematic or repeat violations. A data custodian is not subject to statutory damages for an inadvertent technical violation it discovered or disclosed before notice of a claim, notified within fourteen (14) days, and cured within thirty (30) days, except for Tier 1, Tier 2, or Tier 3 data, intentional or reckless violations, primary data brokerage activities, or penalties sought by the enforcing authority.

(d) The enforcing authority may investigate, subpoena, and bring civil actions, accept assurances of voluntary compliance, and obtain injunctions, deletion, disgorgement, a compliance monitor at the data custodian’s expense, and civil penalties of ten thousand dollars ($10,000.00) per negligent violation and twenty-five thousand dollars ($25,000.00) per intentional or reckless violation per affected resident and fifty thousand dollars ($50,000.00) per day for ongoing systematic violations, deposited in the Wyoming Data Protection Fund. It may proceed on a pattern or practice affecting residents collectively. Its action does not bar a private action.

(e) An action under this chapter may be maintained in the district courts of Wyoming based on the injury established by W.S. 34-31-103(c) without regard to whether that injury would satisfy the standing requirements of the courts of the United States. A provision selecting another state’s law, waiving prospectively the substantive rights of this chapter, or eliminating the class remedy is void as against Wyoming public policy; arbitration of individual claims is permitted if it preserves all substantive rights and does not condition arbitration on waiver of the class right.

34-31-108. Commercial practices; data brokers; federal accommodation.

(a) These provisions implement the property rights of this chapter in specific contexts as property remedies and property-protective obligations, not as a separate regulatory scheme. No data custodian shall engage in behavioral advertising directed at a Wyoming resident based on personal data unless, for Tier 4 data, the data owner has granted a specific data license identifying behavioral advertising as an authorized purpose. Behavioral advertising using Tier 2 or Tier 3 data is prohibited regardless of consent. Behavioral advertising using Tier 1 data is absolutely prohibited. Contextual advertising is not restricted.

(b) Every data broker holding personal data of Wyoming residents shall register annually with the enforcing authority on the terms and fees set by rule, supplying its identity, the categories and sources of data held, its purposes, and its deletion mechanism, on penalty of one thousand dollars ($1,000.00) per day; shall honor a deletion request within thirty (30) days subject only to the exceptions of W.S. 34-31-104(f); and shall participate in the centralized deletion mechanism the enforcing authority shall establish within twenty-four (24) months. There is created the Wyoming Data Protection Fund, consisting of civil penalties, registration fees, and appropriations, continuously appropriated to the enforcing authority for enforcement, the registry and deletion mechanism, public education, and technical assistance.

(c) A statutory servitude arises by operation of law only to the extent another law affirmatively requires, as distinguished from permits, the possession, retention, processing, or disclosure of personal data.

(d) A statutory servitude is an encumbrance on the data owner’s property analogous to an easement arising by operation of law; it conveys only the minimum processing authority strictly necessary to satisfy the specific legal obligation that creates it, is non-possessory, temporary, and reversionary, and shall be construed narrowly.

(e) Any processing of personal data beyond the obligation that creates the servitude — including the development, sale, or licensing of individualized derived data, predictive or scoring products, analytical products, or consumer dossiers — is a surcharge upon the servitude, is not authorized by it, and is a trespass to and conversion of the data owner’s property governed by this chapter, unless the applicable law requires the creation and commercial provision of that derived data.

(f) Laws that create a statutory servitude to the extent they expressly authorize as part of the statutory regulatory scheme include, but are not limited to, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act (which does not preempt this chapter, 15 U.S.C. § 6807(b)), the Fair Credit Reporting

Act (15 U.S.C. § 1681t), the Family Educational Rights and Privacy Act, the Children's Online Privacy Protection Act, and state tax and occupational health and safety requirements. This chapter establishes ownership of personal data and does not regulate the assembly, contents, furnishing, permissible purposes, or accuracy of any report governed by federal law; it applies to personal data subject to such law to the fullest extent not specifically preempted.

34-31-109. Applicability; transition; effective dates; severability.

(a) This chapter applies to personal data of Wyoming residents collected, processed, retained, or transferred on or after the enforcement date, and to earlier-collected data subject to transition, by any data custodian regardless of size, revenue, location, or direct relationship. It does not apply to a natural person's personal or household processing; to a government entity under the Data Privacy-Government Entities Act for data governed by that article, except that a government entity selling or transferring data to a private entity is subject to this chapter as to that transfer and may purchase or access commercial data only on lawful process; or to genuinely deidentified data. A private entity processing personal data on behalf of a government entity is a service provider as to that processing and a data custodian as to processing beyond the engagement.

(b) Within twelve (12) months of enactment a data custodian holding earlier-collected data shall identify it, determine whether a valid access authority exists, and obtain authority or complete verifiable deletion; data not brought into compliance is held without valid access authority from the enforcement date, subject to a discretionary extension not exceeding ninety (90) days.

(c) W.S. 34-31-101 through 34-31-102 and the rulemaking and declaration provisions are effective on enactment; the remainder is effective twelve (12) months after enactment as the enforcement date. During the interim, data custodians making good-faith compliance efforts are not civilly liable, the enforcing authority may investigate and accept compliance assurances, and data owners may exercise deletion and access rights.

(d) W.S. 9-21-202(a) is amended by adding: "Nothing in this article limits or is limited by the Wyoming Personal Data Ownership Act, W.S. 34-31-101 through 34-31-109; where both address the same subject, both apply and the more protective provision governs." The Legislative Service Office shall codify and arrange this act.

(e) The declaration and rules of construction in W.S. 34-31-101 are severable from the operative provisions; the property rights of W.S. 34-31-103 and 34-31-104 are severable from the commercial-practice provisions of W.S. 34-31-108; and each tier is severable from the others. If the statutory servitude framework of W.S. 34-31-108 is held invalid as to any law, this chapter applies to the fullest extent that law permits.

(END OF ACT)

Wyoming Personal Data Ownership Act — Draft Version Alt-21.7 (Consolidated) — W.S. 34-31-101 through 34-31-109 — July 2026