DRAFT ONLY
NOT APPROVED FOR INTRODUCTION

HOUSE BILL NO.

Wyoming Personal Data Ownership Act.

Sponsored by: Select Committee on Blockchain, Financial Technology and Digital Innovation Technology

A BILL

for

AN ACT relating to property, conveyances and security transactions; classifying personal data as intangible personal property; classifying personal data into tiers; specifying protections for personal data; establishing ownership rights in personal data; providing access authority for personal data; establishing rights of data owners; providing duties of data custodians; requiring registration of data brokers; requiring the secretary of state to establish a centralized deletion mechanism for personal data held by data brokers; providing a civil cause of action; specifying and authorizing remedies; providing civil penalties; amending the Wyoming Governmental Claims

Act; providing definitions; making conforming amendments; requiring rulemaking; specifying applicability; and providing for effective dates.

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

****

STAFF COMMENT

The Select Committee may wish to consider the broader legal and practical implications of classifying personal data as intangible personal property and granting data owners full property rights in that data. This approach would represent a significant change from existing privacy and consumer protection frameworks, which generally regulate the collection, use, disclosure, and retention of personal data without necessarily treating the data itself as property owned by an individual. By creating a property-rights framework, this bill draft may affect how courts, regulated entities, government entities, and data owners understand ownership, possession, licensing, transfer, inheritance, remedies, and enforcement with respect to personal data. Because of the nuance and complexity of the property and rights at issue, this bill draft may have unintended consequences.

The Select Committee may wish to consider whether additional clarification is necessary regarding the scope and boundaries of the ownership interest in personal data that is being created. For example, the bill draft may raise questions regarding when personal data is created, who owns personal data relating to more than one person and how the ownership interest applies when another person has lawfully collected, possessed, processed, or relied on the data before the effective date of this act.

Because this bill draft would create a new statutory property-rights framework for personal data, there may be

legal, operational or practical consequences that cannot be fully identified or anticipated in advance.
****

Section 1. W.S. 1-39-125, 34-31-101 through 34-31-115 and 34-31-117 are created to read:

1-39-125. Liability; Wyoming Personal Data Ownership Act.

A governmental entity is liable for damages resulting from a violation of the Wyoming Personal Data Ownership Act.

CHAPTER 31

WYOMING PERSONAL DATA OWNERSHIP ACT

34-31-101. Short title.

This chapter shall be known and may be cited as the "Wyoming Personal Data Ownership Act."

34-31-102. Purposes; construction.

****

STAFF COMMENT

The Select Committee may wish to consider whether this purpose section is necessary.

****

(a) The purpose of this chapter is to recognize that personal data constitutes intangible personal property of the data owner and to protect the ownership interest of Wyoming residents in their personal data as provided by this chapter.

(b) This chapter shall not be construed to:

(i) Authorize the permanent alienation or waiver of any ownership interest in personal data or non-waivable right established under this chapter;

****

STAFF COMMENT

The Select Committee may wish to consider whether paragraph (b)(i) reflects the intended limitation on a data owner's ability to permanently transfer personal data. As drafted, the paragraph appears to prohibit a data owner from permanently selling, assigning, or waiving the data owner's title to personal data or ownership interest in personal data, even if the data owner voluntarily agrees to do so. If the result is not intended, the Select Committee may wish to consider whether permanent transfers should be

allowed to some personal data or under specified safeguards.
****
****

(ii) Regulate, restrict or impose liability for expression, expressive conduct or expressive association protected by the first amendment to the United States constitution, Article 1, Section 20 of the Wyoming constitution or Article 1, Section 21 of the Wyoming constitution;

(iii) Authorize a government entity to acquire personal data through a legal process that is not otherwise authorized by law or to reduce or limit any requirement imposed on a government entity under W.S. 9-21-201 through 9-21-203;

(iv) Restrict access to information required to be available for public inspection under the Public Records Act;

(v) Preclude or limit any common law claim relating to property or personal data or remedy otherwise available under law.

(c) No person shall avoid the requirements of this chapter by using a form, label, contractual characterization, affiliate relationship, intermediary, organizational structure or transaction structure that has the purpose or effect of evading or circumventing this chapter. In applying this chapter, the substance and practical effect of a person's conduct, transaction, arrangement, relationship or course of dealing shall control over the form, label or characterization used by the person.

(d) No person shall avoid classification as a data custodian or a service provider under this chapter by using, directing, controlling, deploying or making available an artificial intelligence system or automated system to process personal data. For purposes of this chapter, a person that uses, directs, controls, deploys or makes available an artificial intelligence system or automated system to process personal data shall be subject to the duties, liabilities and obligations applicable to that person under this chapter.

****

STAFF COMMENT

The Select Committee may wish to consider whether subsection (d) sufficiently addresses artificial intelligence systems and automated systems under the Wyoming Personal Data Ownership Act. As drafted, an artificial intelligence system itself may not be a "person" and therefore may not independently qualify as a data custodian or service provider. Subsection (d) is intended to clarify that a person may not avoid duties, liabilities or obligations under this chapter by using, directing, controlling, deploying or making available an artificial intelligence system or automated system to process personal data.

****

34-31-103. Definitions.

(a) As used in this chapter:

(i) "Access authority" means a data license, owner-granted authorization or lawful use that authorizes the processing of personal data under this chapter for an authorized purpose;

(ii) "Affirmative consent" means consent that is freely given, specific, informed, unambiguous and revocable. "Affirmative consent" shall not include silence, pre-checked boxes, default settings, non-negotiable terms,

continued use or any action obtained through a dark pattern;

(iii) "Authorized purpose" means the purpose for processing personal data that is expressly authorized by an access authority, statutory servitude, employment data authorization, court order, warrant or other authorization expressly provided under this chapter or other applicable law;

(iv) "Authorized representative" means any of the following:

(A) A parent or legal guardian of a data owner who is a minor;

(B) A personal representative of a deceased data owner's estate;

(C) A person who has been granted a power of attorney by a data owner and who is expressly authorized to exercise rights on behalf of the data owner under this chapter;

(D) A court appointed guardian or conservator.

(v) "Behavioral advertising" means the selection or delivery of an advertisement to a data owner based on personal data obtained or inferred from the data owner's activities over time or across nonaffiliated websites, applications, services or devices. "Behavioral advertising" shall not include contextual advertising;

(vi) "Biometric identifier" means data generated from one (1) or more biological, physiological or behavioral characteristics of a natural person that is used or reasonably capable of being used to identify a specific natural person, including a fingerprint, palm print, voiceprint, vocal biomarkers, eye retina or iris scan, hand geometry, facial geometry or templates, gait patterns or rhythms or any other biological, physiological or behavioral characteristic that is used to identify a specific natural person. "Biometric identifier" shall not include:

(A) A physical or digital photograph or data derived from a physical or digital photograph, unless the photograph or derived data is processed or retained for processing to generate a biometric identifier, in whole or in part, for the purpose of identifying or verifying the identity of a specific natural person;

(B) A video or audio recording or data derived from a video or audio recording, unless the video or audio recording or derived data is processed or retained for processing to generate a biometric identifier, in whole or in part, for the purpose of identifying or verifying the identity of a specific natural person.

(vii) "Commercial exploitation" means processing personal data primarily for monetary gain or other commercial gain, including sales, licensing, behavioral advertising, targeted marketing, profiling for commercial purposes, training of an artificial intelligence or automated system and developing a product or service for commercial distribution. "Commercial exploitation" shall not include:

(A) Any voluntary communication with the data owner that the data owner initiates or terminates;

(B) The creation, production, distribution or promotion of expression or expressive conduct, provided that the personal data used is not sold, transferred or combined with personal data from another source to develop individualized profiles.

****

STAFF COMMENT

The Select Committee may wish to consider whether the definition of "commercial exploitation" is sufficiently clear and whether it appropriately distinguishes between commercial monetization of personal data and ordinary operational processing, customer communications, expressive conduct, and other lawful uses authorized under this chapter.

****

(viii) "Contextual advertising" means the selection or delivery of an advertisement based solely on the content of the website, application, service, search query or transaction that the data owner is currently interacting with. "Contextual advertising" shall not include advertising that uses personal data to identify,

profile or target the data owner over time or across nonaffiliated websites, applications, services or devices;

(ix) "Dark pattern" means a user interface or choice architecture that is designed or has the reasonably foreseeable effect of materially subverting, impairing or interfering with a data owner's autonomy, decision-making or choice regarding the processing of personal data;

(x) "Data broker" means a data custodian who, in the ordinary course of business, knowingly collects, aggregates, sells, licenses, transfers or provides access to personal data of persons with whom the data custodian does not have a direct relationship if the sale, licensing, transfer or provision of access to that personal data is a material part of the data custodian's business;

(xi) "Data custodian" means any person that processes or derives commercial value from the personal data of a data owner, regardless of the location of the person or of any direct relationship with the data owner. "Data custodian" shall not include a person who solely provides passive technical infrastructure and does not

determine the purpose of processing or deriving commercial value from the personal data;

****

STAFF COMMENT

As currently drafted, the definition of "data custodian" applies regardless of the person's location or whether the person has a direct relationship with the data owner. This is intended to conform the bill draft to a property-rights framework by treating the data owner's ownership interest in personal data as continuing despite disclosure, copying, transfer, processing, or possession by another person outside of Wyoming. Under this approach, the data owner's property right follows the personal data and is not extinguished based on the location of the person holding or processing the personal data.

The Select Committee may wish to consider whether applying the definition regardless of the location of the person creates any legal issue regarding personal jurisdiction, due process, and extraterritorial application. A court may require a showing that an out-of-state person has sufficient contacts with Wyoming or has purposefully directed conduct toward Wyoming residents before the chapter can be enforced against that person. The Select Committee may wish to consider whether to retain the "regardless of the location" standard to reflect the intended property-rights approach or whether to add a Wyoming nexus requirement to reduce potential constitutional challenges.

****

(xii) "Data license" means an authorization, agreement or instrument granted or purportedly granted by the data owner to permit the processing of specified

personal data for an authorized purpose in accordance with the requirements of W.S. 34-31-111;

(xiii) "Data owner" means a natural person who is a Wyoming resident and to whom personal data relates or to whom personal data is linked or reasonably linkable;

(xiv) "Deidentified data" means data that cannot reasonably be used, alone or in combination with other information reasonably available under generally accepted technical, administrative and organizational standards, to identify, infer information about or otherwise be linked to a specific natural person, personal digital identity or device linked to a natural person or personal digital identity. Removal of direct identifiers alone shall be insufficient to constitute deidentified data;

****

STAFF COMMENT

This definition differs from the definition of "deidentified data" in W.S. 9-21-201(a)(i). The Select Committee may wish to consider whether the definition of "deidentified data" in this bill draft should be conformed to W.S. 9-21-201(a)(i), whether W.S. 9-21-201(a)(i) should be amended to conform to this bill draft, or whether the Select Committee intends differing definitions.

9-21-201. Definitions.

(a) As used in this article:

(i) "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person or personal digital identity or a device linked to a natural person or personal digital identity;

****

(xv) "Derived data" means data, information, inference, prediction, score, classification, profile or other output that is created, generated or inferred through a computational, statistical or inferential process applied to personal data, whether alone or in combination with other data, and that is linked or reasonably linkable to an identified or identifiable natural person or personal digital identity. "Derived data" shall not include a generalized model, model weights, aggregate data or deidentified data;

(xvi) "Financial account data" means information concerning a natural person's financial accounts, payment credentials, account numbers, account access credentials, transaction history, account balances or financial holdings;

(xvii) "Geolocation data" means information derived from technology that identifies or is reasonably capable of identifying the present or past physical location of a natural person or device of a natural person with sufficient precision to locate the natural person or device within a radius of one thousand seven hundred fifty (1,750) feet;

(xviii) "Government entity" means the state and all its political subdivisions, agencies, instrumentalities and institutions and any local government entity and its agencies, instrumentalities and institutions;

****
STAFF COMMENT
This definition of "government entity" is broader than the definition of "government entity" in W.S. 9-21-201(a)(ii). W.S. 9-21-201(a)(ii) expressly excludes the judicial branch of government and any law enforcement agency in Wyoming. This bill draft does not exclude those entities in order to apply more broadly to all state and local governmental entities. The Select Committee may wish to consider whether the broader definition is intended and whether any conforming language is necessary to clarify the relationship between this chapter and W.S. 9-21-201 through 9-21-203.

9-21-201. Definitions.

(a) As used in this article:

(ii) "Government entity" means the state and all its political subdivisions, agencies, instrumentalities and institutions and any local government entity. "Government entity" shall not include the judicial branch of government or any law enforcement agency in Wyoming;

****

(xix) "Identified or identifiable natural person" means a natural person who is identified or who can reasonably be identified, directly or indirectly, by reference to an identifier, personal digital identity or other information that, alone or in combination with other reasonably available information, links or is reasonably linkable to the natural person;

****

STAFF COMMENT

This definition differs from the definition of "identified or identifiable natural person" in W.S. 9-21-201(a)(iii). The definition in this bill draft appears to more closely conform to the bill draft's use of "reasonably linkable" and its references to personal digital identity. The Select Committee may wish to consider whether to retain the definition in this bill draft for internal consistency, conform the definition to W.S. 9-21-201(a)(iii), amend W.S. 9-21-201(a)(iii) to conform to this bill draft, or whether the Select Committee intends differing definitions.

9-21-201. Definitions.

(a) As used in this article:

(iii) "Identified or identifiable natural person" means a natural person who can be readily identified, directly or indirectly, by reference to an identifier such as a name, an identification number, specific geolocation data or an online identifier;

****

(xx) "Individualized derived data" means derived data that is linked or reasonably linkable to an identified or identifiable natural person or to a personal digital identity;

(xxi) "Lawful use" means a statutory, non-possessory privilege created under W.S. 34-31-111 that authorizes processing of personal data for an authorized purpose without a data license, owner-granted authorization, user-directed disclosure or any other authorization from the data owner;

(xxii) "Minimum necessary" means the least amount and least identifying form of personal data sufficient to accomplish the authorized purpose under the applicable access authority or statutory servitude, considering the highest tier classification applicable to the personal data under W.S. 34-31-105;

****

STAFF COMMENT

The Select Committee may wish to consider whether the definition of "minimum necessary" provides sufficient guidance for data custodians and courts. The definition requires use of the least amount and least identifying form of personal data sufficient to accomplish the authorized purpose, but it may be unclear how that standard will be applied in different operational, technical, or legal contexts. The Select Committee may wish to consider whether additional objective factors should be included.

****

(xxiii) "Minor" means a natural person under the age of eighteen (18) years;

(xxiv) "Neural data" means information that is generated by measuring the activity of a natural person's central or peripheral nervous system and that is not inferred from nonneural information;

****

STAFF COMMENT

The definition of "neural data" is from the definition of "neural data" in the California Consumer Privacy Act of 2018. The Select Committee may wish to consider whether that definition is appropriate for this bill draft or whether it should be revised to better fit Wyoming's property-rights framework for personal data.

****

(xxv) "Owner-granted authorization" means a voluntary, non-assignable permission granted or purportedly granted by a data owner or authorized representative under W.S. 34-31-111 to an identified recipient for an authorized noncommercial purpose. "Owner-granted authorization" shall not include a data license or a user-directed disclosure;

(xxvi) "Personal data" means information that is linked or reasonably linkable to an identified or identifiable natural person or to a personal digital identity. "Personal data" shall include individualized derived data but shall not include deidentified data;

****

STAFF COMMENT

For the Select Committee's reference, "personal digital identity" is not defined in this bill draft because it is defined in W.S. 8-1-102(a)(xviii). Under W.S. 8-1-102(a), that definition applies to all Wyoming statutes unless the Legislature clearly specifies a different meaning or interpretation or the context clearly requires a different meaning.

8-1-102. Definitions.

(a) As used in the statutes unless the legislature clearly specifies a different meaning or interpretation or the context clearly requires a different meaning:

(xviii) "Personal digital identity" means the intangible digital representation of, by and for a natural person, over which he has principal authority and through which he intentionally communicates or acts;

****

(xxvii) "Personal health data" means information relating to the past, present or future physical or mental health condition of a natural person, the provision of health care to a natural person or payment for health care. "Personal health data" shall include health-related personal data collected, processed or maintained by a person that is not a covered entity or business associate under the federal Health Insurance Portability and Accountability Act;

(xxviii) "Processing" means any operation on personal data, including collection, retention, storage, use, disclosure, transmission, sale, transfer, combination, training of an artificial intelligence or automated system, erasure and destruction. "Processing" shall not include transient technical operations or user-directed disclosures. For purposes of this paragraph, "transient technical operations" shall include transient packet routing, signal maintenance, domain resolution, standard

security monitoring and transient caching, if no behavioral profile is created, personal data is not retained beyond the duration necessary for the technical function and the personal data is not used for a commercial purpose;

(xxix) "Published personal expression" means expressive content created, authorized or intentionally made publicly available for public consumption by the data owner or by the owner of the personal expression;

(xxx) "Reasonably linkable" means, with respect to data or information, that the data or information can reasonably be used alone or in combination with other reasonably available information to identify or contact a specific natural person or to associate the data or information with a specific natural person or personal digital identity. Aggregation, transformation, derivation, inference or encoding shall not eliminate linkability if the resulting data or information remains capable of being used to identify or contact a specific natural person or to be associated with a specific natural person or personal digital identity;

(xxxi) "Right of reversion" means the right to terminate all processing authority held by a data custodian as provided in W.S. 34-31-109;

(xxxii) "Sensitive data" means:

(A) Biometric identifiers;

(B) Genetic data;

(C) Neural data;

(D) Personal health data;

(E) Geolocation data;

(F) Religious belief data;

(G) Political affiliation data;

(H) Financial account data;

(J) Personal data of a minor;

(K) Personal data that, if disclosed, would create a substantial risk of physical harm, harassment, intimidation, persecution, discrimination, deprivation of liberty or legal rights or targeting of a natural person or the natural person's lawful property. For purposes of this subparagraph, a substantial risk may arise from the collection, aggregation or commercial availability of the personal data and is not limited to a subsequent use or disclosure of the personal data. A data owner shall not be required to demonstrate that misuse has occurred.

****

STAFF COMMENT

The Select Committee may wish to consider whether additional definitions are needed for the categories of "sensitive data" listed in this paragraph. Several categories, including "genetic data," "religious belief data," and "political affiliation data" are not separately defined in this bill draft.

The Select Committee may wish to consider whether those terms are sufficiently understood in context or whether definitions should be added to assist data custodians, data owners, and courts in consistently determining when personal data falls within a sensitive data category.

The Select Committee may wish to consider whether the substantial-risk category of "sensitive data" provides sufficient guidance. This category includes personal data that, if disclosed, would create a substantial risk of physical harm, harassment, intimidation, persecution,

discrimination, deprivation of liberty or legal rights or targeting. The Select Committee may wish to consider whether additional limiting language is needed, such as requiring the risk to be reasonably foreseeable, substantial and tied to unlawful conduct or objective circumstances.
****

(xxxiii) "Service provider" means a person that processes personal data on behalf of and under the instruction of a data custodian pursuant to a written agreement;

(xxxiv) "Statutory servitude" means the limited, non-possessory authority to process personal data arising by operation of law as provided in W.S. 34-31-110;

(xxxv) "Transfer" means any disclosure, assignment or sharing of personal data with a third-party. "Transfer" shall not include a disclosure to a service provider or a user-directed disclosure;

(xxxvi) "User-directed disclosure" means a specific disclosure of personal data initiated and controlled by the data owner and made as an exercise of the data owner's property right;

(xxxvii) "Verifiable deletion" means the removal, destruction or deidentification of personal data and individualized derived data from active systems and from archives, backups and service providers under a data custodian's control within the time required by this chapter, so that the data is no longer reasonably accessible, recoverable or reasonably linkable to an identified or identifiable natural person, except to the extent retention is required or authorized by law;

(xxxviii) "Wyoming resident" means a natural person domiciled in Wyoming at the time the natural person's personal data is collected, processed or transferred or at the time a right under this chapter is asserted.

34-31-104. Personal data classified as intangible personal property.

****
****

STAFF COMMENT

The Select Committee may wish to consider whether classifying personal data as intangible personal property

may create uncertainty regarding how courts will apply traditional property law concepts, including the Takings Clause of the United States Constitution, to personal data. Because courts may not have existing guidance on how traditional property law doctrines apply to a newly created statutory property interest in personal data, the Select Committee may wish to consider whether additional language is needed to clarify the scope of the property interest and the effect of the act on personal data previously collected, retained, copied, processed, or commercially used by another person before the effective date of this act.
****

(a) Personal data constitutes intangible personal property of the data owner.

(b) Title to personal data vests in the data owner when the personal data is created, collected, generated, derived or becomes linked or reasonably linkable to the data owner and remains continuously vested in the data owner. Title to personal data is not alienable, assignable or transferable during the data owner's life and may pass only by inheritance or succession as provided by law. Nothing in this subsection shall prohibit a data owner from granting access authority or directing a user-directed disclosure as provided by this chapter. Except for the limited processing authority expressly authorized under this chapter, no processing of personal data shall convey,

assign, transfer, waive, alienate or otherwise affect title to the personal data or any ownership interest in the personal data.

(c) Personal data shall constitute intangible personal property under this chapter but shall not constitute a general intangible as defined by W.S. 34.1-9-102(a)(xlii), investment property as defined by W.S. 34.1-9-102(a)(xlix) or money as defined by W.S. 34.1-1-201(a)(xxiv) under title 34.1 of the Wyoming statutes. Personal data shall not be subject to the Uniform Commercial Code-Secured Transactions and shall not be classified as abandoned or unclaimed property. Personal data shall be distinct from digital assets governed by W.S. 34-29-101 through 34-29-107.

(d) The property right recognized under this section shall be enforceable against any person who collects, processes, retains, transfers or derives commercial value from the personal data of a data owner in violation of this chapter. For purposes of enforcing this chapter, an ownership interest in personal data held by a data owner is deemed an intangible personal property interest of a

Wyoming resident and interference with that interest constitutes injury to property of a Wyoming resident.

(e) Unauthorized processing, retention or transfer of personal data in violation of this chapter constitutes a legally cognizable injury to the data owner's property interest in personal data and is actionable without proof of physical harm or economic loss separate from the interference.

****

STAFF COMMENT

The Select Committee may wish to consider whether to amend subsection (e). This subsection provides that unauthorized processing, retention, or transfer of personal data in violation of this chapter constitutes a legally cognizable injury to the data owner's property interest and is actionable without proof of physical harm, economic loss or other damages separate from interference.

A legally cognizable injury is an injury recognized by law as sufficient to support a remedy. In many property contexts, damages generally require a showing of a compensable injury, loss, deprivation, or interference for which monetary or equitable relief may be substituted.

As drafted, subsection (e) appears to treat the statutory interference with personal data itself as the injury, which may provide personal data with remedies or protections that are broader than those available for some other forms of property. The Select Committee may wish to consider whether that result is intended and whether additional limitations, damages provisions, proof requirements, or remedial standards should apply.

****

(f) Individualized derived data shall constitute personal data of the data owner and shall be owned by the data owner. Synthetic data shall be considered personal data under this chapter only to the extent that the synthetic data is reasonably linkable to an identified or identifiable data owner or to a personal digital identity.

****

STAFF COMMENT

The Select Committee may wish to consider defining "synthetic data." Below is a potential definition for the Select Committee's consideration:

"Synthetic data" means artificially generated data that does not directly contain personal data but that is created to resemble, simulate or statistically represent data relating to natural persons or personal digital identifiers.

****

(g) The public availability of personal data shall not diminish the data owner's ownership interest in the personal data. Ownership of personal data shall 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 a data owner, provided that the processing of the personal data does not create individualized derived data for commercial exploitation or otherwise constitute commercial exploitation of the data owner's personal data. The incidental depiction of a natural person in an expressive work shall not, by itself, create individualized derived data, constitute commercial exploitation or require access authority. Information that is not reasonably linkable to an identified or identifiable natural person or personal digital identity shall not constitute personal data and title to that information shall not vest in a data owner. The aggregation or resale of publicly available personal data for commercial exploitation shall be subject to this chapter.

(h) No processing of published personal expression shall require access authority under this chapter unless the processing does or results in one (1) or more of the following:

(i) Uses the data owner's identity or identifying attributes as the basis for identifying, profiling,

impersonating, contacting, locating or making a decision concerning the data owner;

(ii) Produces an output that is attributable to the data owner or that impersonates the data owner;

(iii) Creates or derives a profile reasonably linkable to the data owner;

(iv) Constitutes commercial exploitation of the data owner's personal data.

(j) No access authority or statutory servitude shall convey title to personal data or create any ownership, possessory, equitable, transferable or continuing interest in personal data in the holder. Processing under an access authority or statutory servitude shall be limited to the authorized purpose or purposes.

34-31-105. Classification of personal data.

(a) Ownership interests shall be uniform across all tiers of personal data. There shall be a tier

classification of personal data that governs licensing, transfer and remedies but the tier classification shall not affect the nature or quality of the ownership interest. Tier one (1) personal data shall be the most restrictive tier classification and tier four (4) shall be the least restrictive tier classification. If personal data falls within more than one (1) tier, the personal data shall be subject to the requirements and limitations of the most restrictive applicable tier classification specified in this section.

(b) Personal data shall be classified into the following tiers:

(i) Tier one (1) shall include:

(A) Personal data of a minor who is under thirteen (13) years of age;

(B) Sensitive data limited to genetic data and neural data.

(ii) Tier two (2) shall include:

(A) Personal data of a minor who is between the ages of thirteen (13) and seventeen (17);

(B) Sensitive data limited to personal health data, religious belief data, political affiliation data and financial account data.

(iii) Tier three (3) shall include sensitive data limited to biometric identifiers, geolocation data or personal data that, if disclosed, would create a substantial risk of physical harm, harassment, intimidation, persecution, discrimination, deprivation of liberty or legal rights or targeting of a natural person or the natural person's lawful property;

(iv) Tier four (4) shall include all other personal data.

(c) The following shall apply to each applicable tier of personal data:

(i) Tier one (1) personal data shall be subject to all of the following:

(A) No data license shall authorize processing of tier one (1) personal data for commercial exploitation;

(B) Any instrument, waiver or agreement that purports to authorize processing prohibited under subparagraph (A) of this paragraph shall be void;

(C) Tier one (1) personal data may be processed only pursuant to lawful use, owner-granted authorization or statutory servitude as provided by this chapter. No lawful use or owner-granted authorization shall authorize commercial exploitation of tier one (1) personal data.

(ii) Tier two (2) and tier three (3) personal data shall be subject to all the following:

(A) Tier two (2) and tier three (3) personal data shall be processed only pursuant to access authority or statutory servitude as provided by this chapter;

(B) A data license for tier two (2) and tier three (3) personal data shall require affirmative consent of the data owner and shall be valid for a period of not more than twelve (12) months.

(iii) Tier four (4) personal data shall be subject to all the following:

(A) Tier four (4) personal data shall be processed only pursuant to access authority or statutory servitude as provided by this chapter;

(B) A data license for tier four (4) personal data shall be valid for a period of not more than twenty-four (24) months;

(C) Tier four (4) personal data shall not require affirmative consent unless affirmative consent is otherwise required under this chapter;

(D) No person shall retain tier four (4) personal data for more than three (3) years, unless authorized by access authority, statutory servitude or other law.

(d) If personal data is not disclosed or processed pursuant to access authority, statutory servitude, user-directed disclosure or other authorization expressly provided under this chapter, personal data shall be obtained only through the following legal process:

(i) For a criminal investigation, criminal prosecution or law enforcement purposes, personal data shall be obtained only pursuant to a warrant issued by a court of competent jurisdiction;

(ii) For a civil action, administrative proceeding, regulatory proceeding or other noncriminal action or proceeding, personal data shall be obtained only pursuant to a court order issued by a court of competent jurisdiction after notice to the data owner and an opportunity for the data owner to be heard, unless the

court makes specific findings that delayed notice is necessary and appropriate under the circumstances. If notice is delayed under this paragraph, the court order shall require notice to the data owner as soon as delayed notice is no longer necessary, unless notice is otherwise prohibited by law or court order;

(iii) A warrant or court order issued under this subsection shall authorize only the least amount and least identifying form of personal data necessary to accomplish the purpose stated in the warrant or court order and shall not authorize processing beyond the scope of the warrant or court order;

(iv) Nothing in this subsection shall be construed to limit any greater protection, privilege, confidentiality requirement, notice requirement or suppression remedy otherwise provided by law.

34-31-106. Deidentified data.

(a) A qualified independent expert's written determination that data satisfies the definition of

deidentified data shall create a rebuttable presumption that the data is deidentified.

****

STAFF COMMENT

The Select Committee may wish to consider whether the expert-determination provision for deidentified data may be expensive or difficult to administer. The Select Committee may wish to consider whether one determination may apply to a defined dataset, methodology, or processing context rather than requiring a new determination for each processing activity.

****

(b) Any data custodian that maintains the written determination described in subsection (a) of this section, implements ongoing safeguards against reidentification and requires each recipient of deidentified data through a written agreement, not to reidentify the data shall not be liable under this chapter for processing the data as deidentified data, unless the data custodian knew or reasonably should have known that the data no longer satisfied the definition of deidentified data at the time of processing.

(c) Any person that reidentifies deidentified data shall be subject to this chapter as a data custodian with respect to the reidentified data.

34-31-107. Rights of data owners; death of data owners.

(a) Each data owner shall have the following rights against any data custodian, including a data broker:

(i) To assert title to personal data as intangible personal property in accordance with W.S. 34-31-104;

(ii) To obtain, not later than thirty (30) days after submitting a written request to the data custodian, a copy of the data owner's personal data in a structured, commonly used and machine-readable format, to the extent technically feasible. The copy provided under this paragraph shall include personal data from all applicable tier classifications held by the data custodian. The data custodian shall also provide, for the personal data provided under this paragraph, a description of each

purpose, whether authorized or unauthorized, for which the personal data was obtained or processed and each transferee to whom the personal data was transferred;

(iii) To object in writing to a data custodian that processes the data owner's personal data, to the accuracy, completeness, pertinence or continued processing of the personal data. A data custodian that receives the objection shall verify the identity of the data owner and investigate the objection not later than sixty (60) days after receiving the objection. If the objection is supported, the data custodian shall correct, restrict or delete the data owner's personal data not later than thirty (30) days after completing the investigation, except to the extent the processing is required or authorized by law and shall notify the data owner in writing of the correction, restriction or deletion completed or the specific legal basis for any denial, limitation or delay. If the objection is not supported, the data custodian shall notify the data owner, in writing, of the determination and shall allow a statement of the data owner's position to be maintained with the personal data subject to the objection;

(iv) To demand, in writing, verifiable deletion of personal data at any time. The data custodian shall complete verifiable deletion of a data owner's personal data that is held by or under the possession, custody or control of the data custodian not later than thirty (30) days after receiving the written demand. If personal data has been disclosed to or is maintained by a service provider acting on behalf of and under the direction of the data custodian, the data custodian shall take reasonable steps to require the service provider to complete verifiable deletion not later than thirty (30) days after the data custodian receives the written demand. If deletion is denied, limited, delayed or incomplete because the data custodian has active access authority or a statutory servitude, is otherwise required or permitted by law to retain the personal data or the personal data is not within the possession, custody or control of the data custodian, the data custodian shall notify the data owner, in writing, of the specific basis for the denial, limitation, delay or incomplete verifiable deletion not later than thirty (30) days after receiving the written demand for verifiable deletion;

****

STAFF COMMENT

The Select Committee may wish to consider whether paragraph (a)(iv) provides a realistic and administrable process for verifiable deletion.

****

(v) To revoke any data license issued to a data custodian, at any time, through a clear, conspicuous and reasonably accessible mechanism that is no more burdensome than the mechanism used to grant the data license. Revocation shall not waive any accrued contractual obligation or authorize any penalty, fee or charge imposed solely because the data owner revoked the data license;

(vi) To obtain from the data custodian, upon written request, a description of individualized derived data concerning the data owner that is held by or under the possession, custody or control of the data custodian and to demand, in writing, verifiable deletion of individualized derived data. The data custodian shall provide the description not later than thirty (30) days after receiving the written request. If the data owner demands verifiable deletion, the data custodian shall complete verifiable deletion of individualized derived data that is held by or

under the possession, custody or control of the data custodian not later than thirty (30) days after receiving the written demand, unless retention is authorized by active access authority, statutory servitude or other law. If individualized derived data has been disclosed to or is maintained by a service provider acting on behalf of and under the direction of the data custodian, the data custodian shall take reasonable steps to require the service provider to complete verifiable deletion not later than thirty (30) days after the data custodian receives the written demand. If deletion is denied, limited, delayed or incomplete, the data custodian shall notify the data owner, in writing, of the specific basis for the denial, limitation, delay or incomplete deletion not later than thirty (30) days after receiving the written demand;

(vii) To direct a data custodian, by written request, to make a user-directed disclosure of the data owner's personal data to a person identified by the data owner. A data custodian shall, after verifying the identity of the data owner and the identity, account or delivery destination of the person identified by the data owner, make the user-directed disclosure not later than thirty

(30) days after receiving the written request, in a structured commonly used and machine-readable format, to the extent technically feasible. A data custodian shall not be required to make a user-directed disclosure to the extent the disclosure is prohibited by law or court order. If a data custodian denies, limits or delays a user-directed disclosure under this paragraph, the data custodian shall notify the data owner, in writing, of the specific basis for the denial, limitation or delay not later than thirty (30) days after receiving the written request;

(viii) To bring a cause of action under W.S. 34-31-117 to enforce the data owner's rights under this chapter against a data custodian, including a data broker or any other person that violates this chapter.

(b) The rights provided under subsection (a) of this section, the right of reversion under W.S. 34-31-109 and the inalienability of tier one (1) personal data shall be nonwaivable rights arising from ownership of personal data under this chapter.

(c) Upon a data owner's death, the rights under this section shall be held for the benefit of the deceased data owner and shall pass with the deceased data owner's ownership interest in personal data as provided by Wyoming law, a will or trust. The rights under this section shall not be separately alienable, assignable or waivable and may be exercised only by an authorized representative or by a successor in interest determined under Wyoming law, a will or trust.

(d) Tier one (1) personal data that is sensitive data limited to genetic data or neural data shall remain protected under this chapter and shall not expire upon the data owner's death or by passage of time. Tier one (1) personal data classified solely because the data owner was a minor under thirteen (13) years of age shall, upon the data owner's death, be classified in the tier otherwise applicable to the content of the personal data.

(e) Except as provided in subsection (d) of this section, the rights under subsection (a) of this section shall terminate seventy-five (75) years after the data owner's death. During that period, the rights under

subsection (a) of this section may be exercised by an authorized representative or by a successor in interest determined under Wyoming law, a will or trust. A successor in interest may grant a data license for commercial use for the deceased data owner's name, voice or likeness if the name, voice or likeness had commercial value at the time of death. If an authorized representative or successor in interest dies, resigns, is removed or otherwise ceases to have authority during the period specified in this subsection, the rights under subsection (a) of this section may be exercised by the next authorized representative or successor in interest determined under Wyoming law, a will or trust.

34-31-108. Digital bailment; duties of data custodians.

(a) For purposes of this chapter, a data custodian that holds, stores, processes or otherwise exercises custody or control over personal data shall owe the data owner the duties specified in this section. Title to the personal data shall remain vested in the data owner. The relationship established under this section is statutory

and shall not be construed to convey title to personal data, to incorporate common law bailment duties, except as expressly provided in this chapter or to preclude or limit any common law property claim or remedy otherwise available under law.

(b) Each data custodian shall owe each data owner whose personal data is held by the data custodian the following duties:

(i) To maintain reasonable safeguards appropriate to the nature and tier of the personal data to protect the personal data against unauthorized processing;

(ii) To process personal data only for authorized purposes and within the scope of the applicable access authority, statutory servitude or other authorization provided under this chapter or other applicable law;

(iii) To collect, retain and process only the minimum necessary personal data for the authorized purpose;

(iv) To maintain reasonable accuracy of personal data to the extent necessary for the authorized purpose of processing and to investigate objections submitted by the data owner under W.S. 34-31-107(a)(iii);

(v) To respond truthfully to access requests not later than thirty (30) days after receiving the request;

(vi) To require, by written agreement, service providers acting on behalf of or under the direction of the data custodian to comply with this chapter and any applicable access authority, statutory servitude or other authorization provided under this chapter or other applicable law. A data custodian shall remain responsible under this chapter for personal data held by or under the possession, custody or control of a service provider acting on behalf of or under the direction of the data custodian;

(vii) To disclose, upon request of the data owner, the tiers of personal data processed, each purpose, whether authorized or unauthorized, for processing and a reasonable estimate of revenue derived from the data owner's personal data.

34-31-109. Automatic termination.

(a) Upon the expiration, revocation, completion or termination of access authority, all processing authority held by a data custodian under the access authority shall terminate automatically. Title to personal data remains continuously vested in the data owner and only the processing authority shall terminate.

(b) Upon the operation of the right of reversion under subsection (a) of this section, the data custodian shall cease processing the data owner's personal data. Except when a statutory servitude requires retention under W.S. 34-31-110, the data custodian shall complete verifiable deletion of the data owner's personal data not later than thirty (30) days after the date the right of reversion occurs and shall notify the data owner of the deletion, in writing, not later than thirty-five (35) days after the date the right of reversion occurs.

(c) After the right of reversion occurs or after a data owner demands verifiable deletion under W.S. 34-31-

107(a)(iv) or (vi), no data custodian shall process or derive value from the data owner's personal data or individualized derived data, except pursuant to active access authority, a statutory servitude or other authorization under this chapter. A violation of this subsection shall constitute unauthorized processing and is subject to the remedies provided by this chapter.

(d) After the right of reversion occurs or after a data owner demands verifiable deletion under W.S. 34-31-107(a)(iv) or (vi), no data custodian shall possess, store or retain the data owner's personal data or individualized derived data except pursuant to active access authority, a statutory servitude or other authorization under this chapter. Storage and retention of the data owner's personal data or individualized derived data shall constitute possession for purposes of this chapter. A violation of this subsection shall constitute unauthorized processing and interference with the data owner's property interest under this chapter and shall be subject to the remedies provided by this chapter.

(e) Revocation of a data license shall operate prospectively and shall not require the recall, alteration or destruction of an expressive work that was created and published before revocation. After revocation of a data license, the data custodian shall not use the personal data to create a new expressive work or new commercial use, except as necessary to complete a transaction previously requested or authorized by the data owner before revocation or as otherwise authorized by law.

34-31-110. Statutory servitude.

(a) A statutory servitude shall arise by operation of law only to the extent necessary for a data custodian to comply with a specific obligation imposed by state or federal law that affirmatively requires the processing of personal data. A law that merely permits, authorizes or does not prohibit processing of personal data shall not create a statutory servitude.

(b) A statutory servitude shall be a limited encumbrance on the data owner's ownership interest in personal data and shall be construed narrowly. A statutory

servitude shall be non-possessory, temporary and reversionary.

(c) No statutory servitude shall authorize any processing of personal data or individualized derived data beyond the obligation imposed by the law giving rise to the statutory servitude. The creation, retention or use of individualized derived data under a statutory servitude shall be permitted only to the extent expressly required by the law giving rise to the statutory servitude. The sale, license, transfer or commercial provision of individualized derived data, predictive or scoring products, analytical products, consumer dossiers or substantially similar products shall be outside the scope of the statutory servitude and shall constitute unauthorized processing under this chapter, unless the law giving rise to the statutory servitude expressly requires the sale, license, transfer or commercial provision of the individualized derived data or product. Nothing in this subsection shall be construed to prohibit processing that is independently authorized by valid access authority or other authorization under this chapter or other applicable law.

(d) A statutory servitude shall operate on personal data only to the extent and for the duration required by the law giving rise to the statutory servitude and as limited by this section. All tier protections established under W.S. 34-31-105 shall apply to any processing of personal data that is outside the scope or duration of the statutory servitude.

(e) If a data custodian asserts a statutory servitude as a basis to deny, limit or delay verifiable deletion or to continue processing personal data, the data custodian shall notify the data owner, in writing, not later than thirty (30) days after receiving the demand for verifiable deletion or otherwise asserting the statutory servitude. The notice shall specify the state or federal law giving rise to the statutory servitude, the personal data that is subject to the statutory servitude and the processing required by that law, unless notice is prohibited by law or court order.

(f) Upon termination, expiration or satisfaction of the legal obligation giving rise to a statutory servitude, the statutory servitude shall terminate and all processing

authority under the statutory servitude shall cease. Except to the extent retention is otherwise required by law, the data custodian shall complete verifiable deletion of the personal data and any individualized derived data created under the statutory servitude not later than thirty (30) days after the termination of the statutory servitude and shall certify completion of the verifiable deletion to the data owner in writing.

****

STAFF COMMENT

The Select Committee may wish to consider whether the notice and certification requirement in subsection (f) may be burdensome in circumstances where a statutory servitude applies to personal data of many data owners at the same time. The Select Committee may wish to consider whether that result is intended or whether the notice requirement should be limited, modified, or satisfied through a more administrable method, such as notice upon request, representative notice, public notice or another notice process.

****

(g) Nothing in this section shall be construed to regulate the assembly, contents, furnishing, permissible purposes or accuracy of any report, record, disclosure or processing activity to the extent that regulation is prohibited or preempted by federal law. Personal data

subject to requirements of state or federal law shall remain subject to this chapter to the fullest extent permitted by state or federal law and not otherwise prohibited by law. Any statutory servitude arising from those requirements shall extend only to the processing expressly required by the applicable law.

34-31-111. Access authority.

(a) Personal data shall only be processed pursuant to a valid access authority or a statutory servitude as provided by this chapter.

(b) Authorization to process personal data for an authorized purpose shall be construed narrowly and shall not authorize any processing activity that is not expressly stated or reasonably necessary and proportionate to accomplish the authorized purpose.

(c) A data license shall be valid only if the data license:

(i) Is in writing and presented to the data owner in a clear and conspicuous manner separate from general terms and conditions;

(ii) Identifies the specific tiers of personal data subject to the data license, the authorized purpose for processing the personal data and each data custodian or service provider permitted to process the personal data;

(iii) States the duration of the data license, which shall not exceed the applicable maximum duration provided under W.S. 34-31-105(c);

(iv) Separately and conspicuously identifies any authorized transfer, sale, license, disclosure, commercial exploitation or creation of individualized derived data;

(v) Is free of dark patterns;

(vi) Is not conditioned on a product or service in violation of subsection (g) of this section;

(vii) For tier two (2) or tier three (3) personal data, is obtained only by the affirmative consent of the data owner.

(d) A data license that does not satisfy subsection (c) of this section or that contains a term prohibited by subsection (e) of this section shall be void and shall not constitute access authority under this chapter.

(e) A data license shall not:

(i) Authorize the transfer of personal data to an unidentified person, except to a service provider processing personal data on behalf of and under the instructions of the data custodian;

(ii) Contain perpetual, irrevocable or assignable terms;

(iii) Waive any right established under this chapter;

(iv) Require, as a condition of the data license, mediation or arbitration or any other term that waives, limits or impairs any right, cause of action or remedy available under this chapter;

(v) Authorize a government entity to acquire personal data except pursuant to a user-directed disclosure, express written consent when required under W.S. 9-21-202(a) or legal process otherwise authorized by law.

(f) A data custodian asserting access authority under a data license shall bear the burden of proving that the data license is valid under this section. Renewal or extension of a data license shall require new affirmative consent by the data owner if affirmative consent was required for the original data license or is otherwise required under this chapter. An automatic renewal of a data license shall be void.

(g) For purposes of paragraph (c)(vi) of this section, a data license is conditioned on a product or service in violation of this section if the data custodian:

(i) Requires a data license broader than reasonably necessary to provide the product or service;

(ii) Denies an essential product or service because the data owner declines to grant the data license;

(iii) Penalizes the data owner for exercising any right under this chapter.

****

STAFF COMMENT

The Select Committee may wish to consider whether subsection (g) provides sufficient guidance regarding when a data license is improperly conditioned on a product or service. The Select Committee may wish to consider whether additional standards are needed to define "essential product or service," distinguish impermissible coercion from voluntary enhanced features or reduced pricing, and clarify when differences in price, features, limitations, or service levels constitute a penalty.

****

(h) Nothing in subsection (g) of this section shall prohibit a data custodian from offering enhanced features or reduced pricing in exchange for a voluntarily granted data license if the essential product or service remains available to data owners who decline the data license.

(j) An owner-granted authorization shall be separate from and shall not constitute a data license or user-directed disclosure. An owner-granted authorization shall be valid only if the authorization:

(i) Is in writing;

(ii) Identifies the recipient of the authorization, the specific tiers of personal data subject to the authorization and the authorized purpose for processing the personal data;

(iii) Is voluntary;

(iv) Is free of dark patterns.

(k) No owner-granted authorization shall:

(i) Convey title to personal data;

(ii) Create in the recipient any ownership, possessory, equitable, assignable or transferable interest

in personal data or any continuing right to process personal data after completion of the authorized purpose;

(iii) Authorize commercial exploitation, behavioral advertising, profiling, sale, transfer or use of personal data;

(iv) Waive any right, cause of action or remedy available under this chapter.

(m) An owner-granted authorization shall be non-assignable and shall terminate upon completion of the authorized purpose or purposes identified in the authorization. Any arrangement characterized as an owner-granted authorization that involves compensation, assignment, behavioral profiling, sale, transfer or commercial exploitation shall be treated as a data license under this chapter.

(n) An owner-granted authorization may apply to personal data in any tier classification, subject to the requirements and limitations applicable to that tier under W.S. 34-31-105 and this section. An owner-granted

authorization for tier one (1) personal data shall be valid only for a noncommercial purpose and shall not authorize compensation, sale, transfer or commercial exploitation of the tier one (1) personal data. For a minor data owner under thirteen (13) years of age, an authorized representative may grant an owner-granted authorization for tier one (1) personal data only for a noncommercial health, safety, treatment, care coordination or public health purpose directly related to the minor data owner or for noncommercial research or support activities concerning persons with the same disease or medical condition as the minor data owner if an institutional review board with authority to review the research or activity has determined that the research or activity is appropriate, uses the minimum necessary personal data and includes reasonable protections for the minor data owner.

(o) A user-directed disclosure shall be an exercise of the data owner's ownership interest in personal data and shall not constitute a data license or owner-granted authorization. A user-directed disclosure shall not convey title to personal data or authorize the recipient to

process the personal data beyond the specific disclosure directed by the data owner.

(p) A lawful use shall be one (1) form of access authority under this chapter and shall authorize processing without a data license or owner-granted authorization only for the authorized purpose provided under this section. The lawful uses identified in subsection (r) of this section shall not limit the authorized purposes for which a data owner may grant a valid data license or owner-granted authorization under this section. A lawful use shall be a nonpossessory privilege created and governed solely by this chapter. A lawful use shall terminate upon completion of the authorized purpose, whereupon the right of reversion shall operate.

(q) No lawful use shall authorize the commercial exploitation, sale, transfer to a data broker, behavioral advertising, profiling, retention beyond the authorized purpose or commercial processing of tier one (1) personal data. If more than one (1) lawful use applies to the same processing, the data custodian shall satisfy each applicable condition and limitation that provides the

greatest protection to the data owner. No lawful use shall constitute valid access authority if asserted solely to continue possession or retention of personal data without an authorized purpose under this chapter.

(r) The following shall be lawful uses, each of which constitutes an authorized purpose and is limited to the minimum necessary personal data:

(i) Operational necessity, limited to processing strictly necessary to complete a transaction or provide a product or service affirmatively requested by the data owner. Operational necessity may include a continuously operating feature enabled by the data owner if the data owner may disable the feature at any time. Personal data processed under this paragraph shall be subject to verifiable deletion not later than ninety (90) days after completion of the transaction, product, service or enabled feature, unless a statutory servitude requires longer retention. For fraud detection, anti-money-laundering, sanctions screening or substantially similar financial-integrity functions undertaken by a data custodian in connection with a transaction, product, service or enabled

feature requested by the data owner, retention shall be authorized for a period of not more than twenty-four (24) months and the personal data shall be processed only for the documented financial-integrity purpose;

(ii) Personal or household use with no commercial dimension, including making personal content available through an online service, application, website or other medium, if the online service, application, website or medium acts solely as a conduit for the person's own expression and does not process the personal data for commercial exploitation;

(iii) Bona fide journalism, investigative reporting or public-interest accountability concerning a matter of public concern, limited to processing personal data for the specific journalistic, investigative or accountability purpose. A lawful use under this paragraph shall be a single invocation for that purpose;

(iv) Academic or scientific research if the research is approved by an institutional review board with authority to review the research. The institutional review

board shall determine that deidentified data is insufficient for the research purpose. Any participant consent required for the research shall be in writing, approved by the institutional review board and, to the extent applicable, satisfy the definition of affirmative consent under this chapter. A lawful use under this paragraph may include tier one (1) personal data only if the institutional review board with authority to review research determines that the use of tier one (1) personal data is necessary for the research purpose, uses the minimum necessary personal data and includes reasonable protections for the data owner. Personal data may be retained after completion of the research for verification, replication or validation of the research for a period of not more than ten (10) years and only to the extent required by law, a condition of research funding, a publication requirement, an institutional review board requirement or another binding research governance requirement applicable to the research;

(v) Response to an imminent, specific and articulable threat of death or serious physical injury to a data owner or another person, limited to disclosure or

processing reasonably necessary to prevent or mitigate the threat, made only to appropriate emergency medical providers or other persons reasonably able to prevent or mitigate the threat and limited to the duration of the emergency;

(vi) Processing by a professional who is licensed, certified or otherwise authorized under the laws of this state or another jurisdiction to provide the professional service requested or authorized by the data owner, subject to an independent duty of confidentiality and limited to processing necessary to provide that professional service;

(vii) Processing of voter registration data and voluntarily provided contact information for voter registration, voter education, petitioning, civic engagement or communication concerning elections, candidates, ballot measures or political, civic or public affairs. This paragraph shall be construed broadly. Personal data processed under this paragraph shall not be sold, combined for profiling or used for behavioral advertising and shall be subject to verifiable deletion not

later than sixty (60) days after the applicable election, except that voluntarily provided contact information may be retained if the data owner has not demanded verifiable deletion. Nothing in this paragraph shall be construed to authorize a government entity to disclose, transfer or provide access to personal data except as otherwise authorized under W.S. 9-21-201 through 9-21-203, the Public Records Act or other applicable law;

(viii) Professional communication using a person's business contact information provided or published for that purpose, provided that the personal data is not sold, used for profiling or used for behavioral advertising and processing ceases upon the data owner's written request or other clear direction to cease processing;

(ix) Access by a general-purpose search engine or information index to publicly available personal data for indexing, provided that the search engine or information index does not commercially exploit the personal data, aggregate the personal data into personal profiles or make secondary commercial use of the personal data. Incidental

commercial benefit from general indexing shall not constitute commercial exploitation.

34-31-112. Successor transactions; access authority.

(a) Except as provided in subsection (d) of this section, any access authority held by a data custodian shall terminate automatically upon the consummation of a merger, acquisition, sale of substantially all assets, sale under bankruptcy or receivership proceedings, reorganization, change in control or another transaction that results in a successor obtaining control of personal data held by a data custodian. A successor that obtains control of personal data held by a data custodian shall not process the personal data, except as necessary to preserve, secure or return the personal data, to obtain new access authority under this chapter or pursuant to a statutory servitude.

(b) A data custodian shall provide notice to an affected data owner not later than thirty (30) days before consummation of a transaction described in subsection (a) of this section. If prior notice is prohibited by law,

court order or applicable legal confidentiality obligation, the data custodian or successor shall provide notice to the data owner not later than fourteen (14) days after consummation of the transaction.

(c) A successor, purchaser, assignee, trustee, receiver or other transferee shall take personal data subject to the rights of the data owner under this chapter, except to the extent otherwise required by law or court order.

(d) Notwithstanding subsection (a) of this section, a data license or owner-granted authorization for an ongoing product or service that the data owner is actively receiving may continue after consummation of a transaction described in subsection (a) of this section provided that the successor continues the identical product or service on materially identical terms, provides the notice required under subsection (b) of this section and does not process the personal data for any purpose other than the authorized purpose that existed before the transaction. The data license or owner-granted authorization shall terminate upon any material change to the product, service, terms or

authorized purpose of processing or upon revocation by the data owner. For purposes of this subsection, one (1) time transaction records shall not constitute an ongoing product or service.

****

STAFF COMMENT

The Select Committee may wish to consider whether this section appropriately addresses successor transactions, including mergers, affiliate reorganizations, asset sales, bankruptcy sales, receiverships, and changes in control. This section generally terminates existing access authority upon a successor transaction and provides that personal data remains the property of the data owner.

The Select Committee may wish to consider whether this section should distinguish routine continuity-of-service transactions from asset sales or bankruptcy sales, specify what notice must be provided to affected data owners, and clarify whether a successor may temporarily preserve or secure personal data while obtaining new access authority.

The Select Committee may also wish to consider whether this section should be revised to avoid conflicts with federal bankruptcy law, court orders, securities law or other laws governing transfers of business assets.

****

34-31-113. Employment data authorization.

(a) Notwithstanding any other access authority or authorization provided under this chapter, an employment relationship shall create a limited employment data

authorization. The authorized purpose of an employment data authorization shall be to authorize an employer to process an employee's personal data collected or maintained in connection with an employment relationship only to the extent reasonably necessary and proportionate to administer the employment relationship, including payroll, tax reporting, legal compliance, benefits administration, workplace safety, security of employer systems, investigation of suspected misconduct, protection of employer property or confidential information and evaluation of an employee's defined job duties.

(b) An employer that processes employee personal data shall be considered a data custodian under this chapter and shall comply with the duties applicable to a data custodian under this chapter. No employer shall sell employee personal data, transfer employee personal data for commercial exploitation, process employee personal data for a purpose outside the authorized purpose of the employment data authorization or retain employee personal data beyond the employment relationship, except pursuant to a statutory servitude, lawful use, litigation hold, bona fide

employment-related records retention policy or as otherwise authorized by law.

(c) Upon termination of the employment relationship, an employment data authorization provided under this section shall terminate and the right of reversion shall operate, except to the extent retention is required by a statutory servitude, lawful use, litigation hold, bona fide employment-related records retention policy or as otherwise authorized by law.

(d) No employer shall monitor an employee's personal data beyond the scope authorized under subsection (a) of this section. An employer may monitor use of employer-provided applications, employer accounts, employer devices, employer networks and data provided by or stored on employer systems within the scope authorized under subsection (a) of this section, including monitoring reasonably necessary to protect employer systems, investigate suspected misconduct or comply with the law. Monitoring authorized under this subsection shall not authorize an employer to access the contents of an employee's personal account, personal device or personal

communications, even if accessed through an employer provided device, network or system, unless otherwise authorized by law or by a separate owner-granted authorization. Incidental collection of access logs, routing information, security alerts, device identifiers or similar technical information generated by use of an employer provided device, network or system shall not, by itself, constitute access to the contents of an employee's personal account or personal communications.

(e) Nothing in this section shall be construed to limit an employer's ability to comply with federal or state law regarding the collection, retention, disclosure or processing of employee personal data.

****

STAFF COMMENT

The Select Committee may wish to consider whether a separate employment data authorization is necessary or whether employment-related processing should instead be addressed as lawful use under W.S. 34-31-111.

If this section is retained, the Select Committee may wish to clarify the scope of employee personal data covered by this section, the extent to which employers may monitor employer-provided systems and devices, and what employment records may be retained after termination of employment.

****

34-31-114. Behavioral advertising.

(a) No data custodian shall use personal data for behavioral advertising except as authorized under this section.

(b) No behavioral advertising using tier one (1) personal data shall occur. No access authority, waiver or agreement shall authorize behavioral advertising using tier one (1) personal data.

(c) Behavioral advertising using tier two (2), tier three (3) or tier four (4) personal data shall be permitted only under a valid data license that satisfies the requirements of W.S. 34-31-111 and specifically identifies behavioral advertising as an authorized purpose. For tier two (2) or tier three (3) personal data, if the behavioral advertising requires a third-party transfer of the personal data, the data license shall separately authorize the transfer as required under W.S. 34-31-105.

(d) No lawful use or owner-granted authorization shall authorize behavioral advertising.

34-31-115. Data brokers; registration.

(a) Each data broker that holds personal data of a data owner shall annually register with the secretary of state in the form and manner prescribed by the secretary of state in accordance with this section.

(b) The registration required under subsection (a) of this section shall include, at a minimum, the following:

(i) The legal name, trade names and principal address of the data broker;

(ii) The name, mailing address and telephone number of a designated contact for the data broker;

(iii) A description of the tiers of personal data held by the data broker;

(iv) A description of the sources from which the data broker obtains personal data of data owners;

(v) The authorized purposes, if any, for which the data broker processes or otherwise provides access to the personal data;

(vi) A description of the mechanism by which a data owner may demand verifiable deletion of the data owner's personal data;

(vii) Any other information required by rule of the secretary of state that is reasonably necessary to administer this section.

(c) A data broker shall complete verifiable deletion of a data owner's personal data that is held by or under the possession, custody or control of the data broker not later than thirty (30) days after receiving a written demand for verifiable deletion directly from the data owner or a verifiable deletion demand received through the centralized deletion mechanism established under W.S. 34-31-116. If personal data has been disclosed to or is

maintained by a service provider acting on behalf of and under the direction of the data broker, the data broker shall take reasonable steps to require the service provider to complete verifiable deletion not later than thirty (30) days after the data broker receives the written demand or verifiable deletion demand. A data broker may deny, limit or delay deletion only to the extent retention of the personal data is authorized by active access authority, required by a statutory servitude or otherwise required or authorized by law or because the personal data is not within the possession, custody or control of the data broker. A data broker that denies, limits or delays deletion or that cannot complete verifiable deletion shall provide notice to the data owner, in writing, explaining the specific basis for the denial, limitation, delay or incomplete deletion not later than thirty (30) days after receiving the demand for verifiable deletion.

(d) The attorney general may bring a civil action in a court of competent jurisdiction to enforce subsections (a) and (b) of this section and W.S. 34-31-116. In an action brought by the attorney general under this subsection, the attorney general may recover a civil penalty of not more

than one thousand dollars ($1,000.00) for each day that a violation of subsection (a) or (b) of this section or W.S. 34-31-116 continues. Nothing in this subsection shall limit a data owner's private cause of action under W.S. 34-31-117 for a violation of subsection (c) of this section, for a data broker's failure to process a verifiable deletion demand received through the centralized deletion mechanism established under W.S. 34-31-116 or for any unauthorized collection, retention, processing, sale, license, transfer, disclosure or commercial exploitation of the data owner's personal data by a data broker.

34-31-117. Remedies; private cause of action; damages.

(a) A data owner whose rights under this chapter are violated may bring a civil action in a court of competent jurisdiction against a person that violates this chapter. A governmental entity may be liable for damages under this section only to the extent liability is authorized under the Wyoming Governmental Claims Act.

(b) A data owner prevailing in an action under this section may recover actual damages. Except as provided in

subsection (g) of this section, the court may award statutory damages in lieu of actual damages if the court finds that the defendant knowingly, recklessly or willfully violated a data owner's right established under this chapter. Statutory damages shall be awarded once per data owner per action and shall be based on the most protective applicable tier classification of personal data involved in the violation, without separate statutory damages for each record, data element, tier classification or processing activity involved. Statutory damages shall:

(i) For tier one (1) personal data, be not more than fifteen thousand dollars ($15,000.00);

(ii) For tier two (2) personal data, be not more than ten thousand dollars ($10,000.00);

(iii) For tier three (3) personal data, be not more than five thousand dollars ($5,000.00);

(iv) For tier four (4) personal data, be not more than two thousand five hundred dollars ($2,500.00).

****

STAFF COMMENT

The Select Committee may wish to consider whether the statutory damages provisions appropriately reflect the intended level of liability for violations of this chapter. This subsection authorizes statutory damages in lieu of actual damages. Statutory damages are awarded per data owner per action, are based on the most protective applicable tier classification of personal data involved in the violation and are not multiplied based on the number of records or classifications of personal data involved. The Select Committee may wish to consider whether this approach adequately balances deterrence, predictability, and proportionality, particularly in actions involving multiple violations, multiple data owners or large volumes of personal data.

****

(c) In determining whether to award statutory damages and the amount of statutory damages under subsection (b) of this section, the court shall consider the following factors:

(i) The nature, circumstances, extent and gravity of the violation;

(ii) The tier of personal data involved in the violation;

(iii) The number of data owners affected by the violation;

(iv) Whether the violation was committed knowingly, recklessly or willfully;

(v) Whether the defendant acted in good faith;

(vi) Whether the defendant maintained reasonable compliance procedures;

(vii) Whether the defendant cured or attempted to cure the violation;

(viii) Any unjust enrichment obtained by the defendant;

(ix) Any other matter that justice may require.

(d) In addition to damages authorized under this section, a data owner prevailing in an action under this section may recover unjust enrichment obtained by the defendant that is attributable to the unauthorized

processing of the data owner's personal data, except that the court shall avoid duplicative recovery for the same injury or gain and shall not award recovery for unjust enrichment attributable to personal data of persons who are not parties to the action. Unjust enrichment shall be measured by the defendant's actual gain attributable to the unauthorized processing of the data owner's personal data, the fair license value of the data owner's personal data or processing activity at issue, avoided costs attributable to the violation as applied to the data owner's personal data or another equitable measure necessary to prevent the defendant from retaining a benefit obtained by the violation with respect to the data owner's personal data.

****

STAFF COMMENT

The Select Committee may wish to consider whether this subsection provides sufficient standards for calculating unjust enrichment. This subsection permits recovery based on actual gain, fair license value or another measure determined by the court. The Select Committee may wish to consider whether additional guidance should be provided regarding valuation of personal data and individualized derived data to promote consistency and predictability in the assessment of remedies.

****

(e) A court may grant appropriate equitable relief for a violation of this chapter, including injunctive relief,

declaratory relief, verifiable deletion, cessation of unauthorized processing, correction of inaccurate personal data and any other relief necessary to enforce the data owner's rights under this chapter.

(f) A court may award reasonable attorney fees and court costs to a data owner who is a prevailing party in an action under this section.

(g) A purely procedural, technical or notice violation shall not support statutory damages under this section unless the violation results in the unauthorized processing of the data owner's personal data, denial of a verifiable deletion demand or interference with an ownership right established under this chapter. A data owner who is the prevailing party in an action for a violation described in this subsection may recover actual damages, equitable relief and reasonable attorney fees and court costs but shall not recover statutory damages unless the requirements of this section are satisfied.

(h) An action brought under this section is a statutory cause of action. No plaintiff shall be required

to establish any common law property claim to maintain an action under this section.

Section 2. W.S. 34-31-116 is created to read:

34-31-116. Centralized deletion mechanism for data brokers.

(a) The secretary of state, in consultation with the attorney general, shall establish and maintain a centralized deletion mechanism through which a data owner may submit a verifiable deletion demand to one (1) or more registered data brokers.

(b) Each registered data broker shall participate in the centralized deletion mechanism and shall process verifiable deletion demands received through the centralized deletion mechanism in the same manner and within the same time required for a verifiable deletion demand received directly from a data owner under W.S. 34-31-115(c).

(c) Nothing in this section shall limit a data owner's right to submit a verifiable deletion demand directly to a data custodian under W.S. 34-31-107(a)(iv), directly to a data custodian for individualized derived data under W.S. 34-31-107(a)(vi) or directly to a data broker under W.S. 34-31-115(c).

(d) The secretary of state shall adopt rules governing the operation of the centralized deletion mechanism.

****

STAFF COMMENT

As currently drafted, this section is effective immediately in order to provide the Secretary of State time to develop and implement the centralized deletion mechanism before the rest of the act is effective.

****

Section 3. W.S. 1-39-103(a)(ix), 1-39-104(a), 9-21-202(a)(ii) and (d) and 9-21-203(c), as created by 2026 Wyoming Session Laws Chapter 48 and effective July 1, 2027, are amended to read:

1-39-103. Definitions.

(a) As used in this act:

(ix) "This act" means W.S. 1-39-101 through ~~1-39-124~~ 1-39-125.

1-39-104. Granting immunity from tort liability; liability on contracts; exceptions.

(a) A governmental entity and its public employees while acting within the scope of duties are granted immunity from liability for any tort except as provided by W.S. 1-39-105 through 1-39-112 and 1-39-122 through ~~1-39-124~~ 1-39-125. Any immunity in actions based on a contract entered into by a governmental entity is waived except to the extent provided by the contract if the contract was within the powers granted to the entity and was properly executed and except as provided in W.S. 1-39-120(b). The claims procedures of W.S. 1-39-113 apply to contractual claims against governmental entities.

9-21-202. Limitations on personal data by government entities; conflict of laws.

(a) No government entity shall purchase, sell, trade or transfer personal data without the express written consent of the natural person whom the personal data references except as otherwise expressly provided by law and except that:

(ii) A government entity may transfer personal data to a nongovernment entity contracted by the government entity to provide or assist with government services provided by the government entity. Any contract for services with a nongovernment entity shall include requirements for the protection of personal data consistent with this article and, to the extent applicable, with the Wyoming Personal Data Ownership Act. Any personal data transferred pursuant to this paragraph shall be returned or destroyed by the nongovernment entity once the personal data is no longer necessary for the provision of the government service. No nongovernment entity shall maintain, sell, transfer, process or otherwise use the personal data in any manner except as necessary to provide the contracted service and as authorized under this article, the Wyoming Personal Data Ownership Act and any other applicable law;

(d) To the extent that a provision of this article conflicts with another provision of state or federal law, the other provision shall control. Nothing in this article shall be construed to abrogate any disclosure of data or public records under the Wyoming Public Records Act, W.S. 16-4-201 through 16-4-205. Nothing in this article shall be construed to reduce or limit the application of the Wyoming Personal Data Ownership Act to a nongovernment entity, including a nongovernment entity receiving personal data under paragraph (a)(ii) of this section, except to the extent a provision of this article or other law expressly controls. Nothing in the Wyoming Personal Data Ownership Act shall be construed to limit or abrogate the requirements imposed on a government entity under this article.

9-21-203. Personal data collection and retention by government entities.

(c) No government entity shall maintain personal data for longer than three (3) years without a written policy identifying the extended retention period and providing a reasonable justification for the extended retention period.

Statutory retention requirements provided for in W.S. 9-2-405 through 9-2-413 or any other requirement or authorization under law to retain personal data constitute a reasonable justification.

Section 4. This act shall apply to the collection, processing, retention, sale, license, transfer, disclosure or commercial exploitation of personal data that occurs on or after the effective date of this act.

Section 5. Nothing in this act shall be construed to impair or alter any existing contracts, agreements or other obligations regarding the personal data of data owners executed before July 1, 2028.

Section 6. The secretary of state shall promulgate all rules necessary to implement this act.

Section 7.

(a) Except as provided in subsection (b) of this section, this act is effective July 1, 2028.

(b) Sections 2, 6 and 7 of this act are effective immediately upon completion of all acts necessary for a bill to become law as provided by Article 4, Section 8 of the Wyoming Constitution.

(END)