State of Arkansas *As Engrossed: S2/27/25 S3/13/25*
95th General Assembly **A Bill**
Regular Session, 2025 SENATE BILL 258

By: Senator C. Penzo
By: Representative S. Meeks

For An Act To Be Entitled

AN ACT TO CREATE THE ARKANSAS DIGITAL RESPONSIBILITY, SAFETY, AND TRUST ACT; AND FOR OTHER PURPOSES.

Subtitle

TO CREATE THE ARKANSAS DIGITAL RESPONSIBILITY, SAFETY, AND TRUST ACT.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:

SECTION 1. Arkansas Code Title 4, is amended to add an additional chapter to read as follows:

CHAPTER 120

ARKANSAS DIGITAL RESPONSIBILITY, SAFETY, AND TRUST ACT

Subchapter 1 — General Provisions

4-120-101. Title.

This chapter shall be known and may be cited as the "Arkansas Digital Responsibility, Safety, and Trust Act".

4-120-102. Legislative findings.

The General Assembly finds that:

(1) Arkansans and Americans have long valued personal privacy as something that serves essential human needs of liberty, personal autonomy, seclusion, family, intimacy, and other relationships, and security;

(2) Privacy safeguards foundational American values of self-

government;

(3) The United States and Arkansas have long protected aspects of personal privacy since the nation's founding, including through the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments to the United States Constitution and Article 2, §§ 2, 6, 8, 10, 15, 21, and 24 of the Arkansas Constitution;

(4) The United States has a history of leadership in privacy rights, passing some of the first privacy laws as early as the eighteenth century and adopting one (1) of the first national privacy and data protection laws globally in addition to the "fair information practice principles" that have influenced laws and privacy practices around the *world;*

(5)(A) The expansion of computers, internet connectivity, mobile telephones, and other digital information and communications technology has magnified the risks to an individual's privacy that can occur from the collection, processing, storage, or dissemination of personal information.

(B) The overwhelming majority of Arkansans and Americans have smartphones equipped with powerful computers, immense storage capacity, arrays of sensors, and the capacity to transmit information around the world instantaneously.

(C) Some people use these devices continuously and use them to store a digital record of nearly every aspect of their lives.

(D) Arkansans increasingly have other "smart devices" such as automobiles, televisions, home appliances, and wearable accessories that collect, process, and transmit information linked to Arkansans and their *activities to entities around the world.*

(E) Participation in modern society necessitates the adoption of technology, and Arkansans who fail to embrace technological advancements face significant competitive disadvantages in education, employment, healthcare access, and economic opportunity;

(6)(A) The personal information of Arkansans and Americans has been used against them to steal their identities, open financial and credit accounts in their names, and do other personal and financial harm.

(B) Troves of Arkansan and American personal information lie in the hands of state adversaries and criminals;

(7) The aggregation of an increasing volume of data among many different entities expands the exposure to malicious actors in cyberspace and

the availability of personal information to such actors;

(8)(A) The risks of harm from privacy violations are significant.

(B) Unwanted or unexpected disclosure of personal information and loss of privacy can have devastating effects for individuals, including financial fraud and loss, identity theft, and the resulting loss of personal time and money, destruction of property, harassment, and even potential physical injury.

(C) Other effects such as reputational or emotional damage can be equally or even more substantial;

(9)(A) With the development of artificial intelligence and machine learning, the potential to use personal and other information in ways that replicate existing social problems has increased in scale.

(B) Algorithms use personal and other information to guide decision-making related to critical issues, such as credit determination, housing advertisements, and hiring processes, and can result in differing accuracy rates;

(10)(A) Individuals need to feel confident that data that relates to them will not be used or shared in ways that can harm themselves, their families, or society.

(B) As such, organizations that collect, use, retain, and share personal information should be subject to meaningful and effective boundaries on such activities, obligated to take reasonable steps to protect the privacy and security of personal information, and required to mitigate privacy risks to the individuals whose data they steward; and

(11)(A) The majority of governments around the world already impose such restrictions on businesses, but Arkansans do not yet have their right to privacy protected.

(B) It is proper for the General Assembly to protect Arkansans' privacy rights, enforce the rights against those who collect, use, retain, and share their personal information, and establish the legislative framework for responsible, safe, and trustworthy technology in Arkansas.

4-120-103. Definitions.

As used in this chapter:

(1) "Affiliate" means a legal entity that:

(A) Controls, is controlled by, or is under common control with another legal entity; or

(B) Shares common branding with another legal entity;

(2) "Authenticate" means to verify through reasonable means that the consumer who is entitled to exercise the consumer's right is the same consumer exercising those consumer rights with respect to the personal data at issue;

(3)(A) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics.

(B) "Biometric data" includes a fingerprint, voiceprint, eye retina or iris scans, or other unique biological pattern or characteristic that is used to identify a specific individual.

(C) "Biometric data" does not include a physical or digital photograph or data generated from a physical or digital photograph, a video or audio recording or data generated from a video or audio recording, or information collected, used, or stored for healthcare treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as it existed on January 1, 2025;

(4) "Business associate" means the same as defined in the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as it existed on January 1, 2025;

(5) "Child" means an individual younger than thirteen (13) years of age;

(6)(A) "Consent" means a clear affirmative act, if referring to a consumer, that signifies a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer.

(B) "Consent" includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

(C) "Consent" does not include:

(i) An acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other unrelated information;

(ii) The hovering over, muting, pausing, or closing a given piece of content; or

(iii) An agreement obtained through the use of dark

patterns;

(7)(A) "Consumer" means an individual who is a resident of this state acting only in an individual or household context.

(B) "Consumer" does not include an individual acting in a commercial or employment context;

(8) "Consumer health data" means any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis;

(9) "Control" means:

(A) The ownership of, or power to vote, more than fifty percent (50%) of the outstanding shares of any class of voting security of a company;

(B) The control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(C) The power to exercise controlling influence over the management of a company;

(10) "Controller" means an individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data;

(11) "Covered entity" has the same meaning as defined in the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as it existed on January 1, 2025;

(12)(A) "Dark pattern" means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice.

(B) "Dark pattern" includes any practice that the Federal Trade Commission refers to as a dark pattern;

(13) "Decision that produces a legal or similarly significant effect concerning a consumer" means a decision made by a controller that results in the provision or denial by the controller of:

(A) Financial and lending services;

(B) Housing, insurance, or healthcare services;

(C) Education enrollment;

(D) Employment opportunities;

(E) Criminal justice; or

(F) Access to basic necessities, such as food and water;

(14) "Deidentified data" means data that cannot reasonably be linked to an identified or identifiable individual or a device linked to that individual;

(15)(A) "Health record" means a written, printed, or electronically recorded material maintained by a healthcare provider in the course of providing healthcare services to an individual that concerns the individual and the services provided.

(B) "Health record" includes:

(i) The substance of any communication made by an individual to a healthcare provider in confidence during or in connection with the provision of healthcare services; or

(ii) Information otherwise acquired by the healthcare provider about an individual in confidence and in connection with healthcare services provided to the individual;

(16) "Healthcare provider" means the same as defined in the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as it existed on January 1, 2025;

(17) "Healthcare services" has the same meaning as provided in 42 U.S.C. § 234(d)(2), as it existed on January 1, 2025;

(18) "Identified" means a consumer who can be readily identified, directly or indirectly;

(19) "Institution of higher education" means:

(A) A vocational or technical school governed by Arkansas Code Title 6, Subtitle 4; or

(B) A postsecondary or higher education institution governed by Arkansas Code Title 6, Subtitle 5;

(20) "Known child" means a child under circumstances where a controller has actual knowledge of, or willfully disregards, the child's age;

(21) "Nonprofit organization" means:

(A) A corporation governed by Arkansas Code Title 4, Chapter 28 or Chapter 33 to extent applicable to nonprofit corporations;

(B) An organization exempt from federal taxation as a nonprofit entity under § 501(a) of the Internal Revenue Code, by being listed as an exempt organization under §§ 501(c)(3), 501(c)(4), 501(c)(6), 501(c)(12), or 501(c)(19) of the Internal Revenue Code; or

(C) A political organization;

(22)(A) "Personal data" means any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual.

(B) "Personal data" includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual.

(C) "Personal data" does not include deidentified data or publicly available information;

(23) "Political organization" means a party, committee, association, fund, or other organization, regardless of whether incorporated, that is organized and operated primarily for the purpose of influencing or attempting to influence:

(A) The selection, nomination, election, or appointment of an individual to federal, state, or local public office or an office in a political organization, regardless of whether the individual is ultimately selected, nominated, elected, or appointed; or

(B) The election of a presidential or vice-presidential elector, regardless of whether the elector is ultimately selected, nominated, elected, or appointed;

(24)(A) "Precise geolocation data" means information derived from technology, including Global Positioning System level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet (1,750').

(B) "Precise geolocation data" does not include the content of communications or any data generated by or connected to an advanced utility metering infrastructure system or to equipment for use by a utility;

(25) "Process" means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data;

(26) "Processor" means a person who processes personal data on behalf of a controller;

(27) "Profiling" means a form of automated processing performed

on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements;

(28) "Protected health information" means the same as defined under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as it existed on January 1, 2025;

(29) "Pseudonymous data" means any information that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual;

(30) "Publicly available information" means information that is lawfully made available through government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted the information to a specific audience;

(31)(A) "Sale of personal data" means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by a controller to a third party.

(B) "Sale of personal data" does not include:

(i) The disclosure of personal data to a processor that processes the personal data on the controller's behalf;

(ii) The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

(iii) The disclosure or transfer of personal data to an affiliate of a controller;

(iv) The disclosure of information that the consumer:

(a) Intentionally made available to the general public through a mass media channel; and

(b) Did not restrict to a specific audience; or

(v) The disclosure or transfer of personal data to a third party as an asset that is part of a merger or acquisition;

(32)(A) "Sensitive data" means a category of personal data.

(B) "Sensitive data" includes:

(i) Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status;

(ii) Genetic or biometric data that is processed for the purpose of uniquely identifying an individual;

(iii) Personal data collected from a known child;

(iv) Precise geolocation data;

(v) Data concerning personal or political affiliations;

(vi) A person's Social Security number, driver's license number, or other government-issued identification number;

(vii) Credentials, that may include a username, login identifier, email address, screen name, or similar identifier in combination with a required security code, access code, or password that would permit access to a consumer's online account;

(viii) Financial information, that may include a consumer's account number, account login, financial account, or credit or debit card number, in combination with a required security code, access code, or password that would permit access to a consumer's online financial account; or

(ix) Consumer health data;

(33) "State agency" means a department, commission, board, office, council, authority, or other agency in any branch of state government that is created by the Arkansas Constitution or a statute of this state, including a university system or institution of higher education as governed by Arkansas Code Title 6, Subtitles 4 or 5 that receives state funding or has *directors appointed by the Governor;*

(34) "Substantial factor" means a factor that: (A) Assists in making a decision that produces a legal or similarly significant effect concerning a consumer;

(B) Is capable of altering the outcome of a decision that produces a legal or similarly significant effect concerning a consumer;

(C) Is generated by an artificial intelligence system; and

(D) Includes any use of an artificial intelligence system to generate any content, decision, prediction, or recommendation concerning a consumer that is used as a basis to make a decision that produces a legal or similarly significant effect concerning a consumer;

(35)(A) "Targeted advertising" means displaying to a consumer an advertisement that is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.

(B) "Targeted advertising" does not include an advertisement that:

(i) Is based on activities within a controller's own websites or online applications;

(ii) Is based on the context of a consumer's current search query, visit to a website, or online application;

(iii) Is directed to a consumer in response to the consumer's request for information or feedback; or

(iv) Is used for the processing of personal data solely for measuring or reporting advertising performance, reach, or frequency;

(36) "Third party" means a person, other than the consumer, the controller, the processor, or an affiliate of the controller or processor; and

(37) "Trade secret" means all forms and types of information, including business, scientific, technical, economic, or engineering information, and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and irrespective of how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

(A) The owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret; and

(B) The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

4-120-104. Applicability.

(a) This chapter applies only to a person that:

(1) Conducts business in this state or produces a product or service consumed by residents of this state;

(2) Processes or engages in the sale of personal data; and

(3) Is not a small business as defined by the United States Small Business Administration, as it existed on January 1, 2025, except to the extent that § 4-120-302(a) applies to a person described by this section.

(b) This chapter shall only apply to nonprofit organizations whose annual receipts in any of the preceding five (5) calendar years exceeded fifteen million dollars ($15,000,000).

4-120-105. Exemptions.

This chapter does not apply to:

(1) A state agency or political subdivision of this state;

(2) A financial institution, affiliates of financial institutions, or data subject to Title V, Gramm-data is collected and used within the context of that role; Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, established under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as it existed on January 1, 2025, and the Health Information Technology for Economic and Clinical Health Act, Division A, Title XIII, and Division B, Title IV, Pub. L. No. 111-5;

(4) An institution of higher education;

(5) An electric utility governed by Arkansas Code Title 23, Chapter 18;

(6) Protected health information under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as it existed on January 1, 2025;

(7) Health records;

(8) Patient identifying information for purposes of 42 U.S.C. § 290dd-2;

(9) Identifiable private information:

(A) For purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46, as it existed on January 1, 2025;

(B) Collected as part of human subjects research under the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or of the protection of human subjects under 21 C.F.R. Parts 50 and 56, as it existed on January 1, 2025; or

(C) That is personal data used or shared in research conducted according to the requirements stated in this chapter or other research conducted according to applicable law;

(10) Information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. § 11101 et seq., as it existed on January 1, 2025;

(11) Patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. § 299b-21 et seq., as it existed on January 1, 2025;

(12) Information derived from any of the healthcare-related information listed in this section that is deidentified according to the requirements for deidentification under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as it existed on January 1, 2025;

(13) Information originating from, intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this section that is maintained by a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. Section 1320d et seq., or by a program or a qualified service organization as defined by 42 U.S.C. Section 290dd-2;

(14) Information that is included in a limited data set as described by 45 C.F.R. Section 164.514(e), as it existed on January 1, 2025, to the extent that the information is used, disclosed, and maintained in the manner specified by 45 C.F.R. Section 164.514(e), as it existed on January 1, 2025;

(15) Information collected or used only for public health activities and purposes as authorized by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as it existed on January 1, 2025;

(16) The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's

creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of the consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t, as it existed on January 1, 2025;

(17) Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq., as it existed on January 1, 2025;

(18) Personal data regulated by the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, as it existed on January 1, 2025;

(19) Personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act of 1971, 12 U.S.C. § 2001 et seq., as it existed on January 1, 2025;

(20) Data processed or maintained in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role, except as specifically provided in § 4-120-602;

(21) Data processed or maintained as the emergency contact information of an individual under this chapter that is used only for emergency contact purposes;

(22) Data that is processed or maintained and is necessary to retain to administer benefits for another individual that relates to an individual described in subdivision (20) of this section and used only for the purposes of administering those benefits;

(23) The processing of personal data by a person in the course *of a purely personal or household activity; or*

(24) Data that is processed or maintained for the sole purpose of detecting, investigating, tracking, reporting, mitigating, or preventing fraudulent or criminal activity, either for the person responsible for the data or on behalf of another person or persons, or assisting law enforcement in any of those activities.

4-120-106. Construction of chapter — Exceptions.

(a) This chapter shall not be construed:

(l) To restrict a controller's or processor's ability to:

(A) Comply with state laws or rules, or federal or local laws, rules, or regulations;

(B) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(C) Investigate, establish, exercise, prepare for, or defend legal claims;

(D) Provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer before entering into a contract;

(E) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis;

(F) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;

(G) Preserve the integrity or security of systems and investigate, report, or prosecute those responsible for breaches of system security;

(H) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similar independent oversight entity that determines:

(i) If the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(ii) Whether or not the expected benefits of the research outweigh the privacy risks; and

(iii) If the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

(I) Assist another controller, processor, or third party with any of the requirements under this section;

(2) As imposing a requirement on controllers and processors that adversely affects the rights or freedoms of any *person or entity,* including the right of free speech; or

(3) As requiring a controller, processor, third party, or consumer to disclose a trade secret.

(b) If personal data is subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data, the requirements imposed on controllers and processors under this chapter may not restrict a controller's or processor's ability to collect, use, or retain data to:

(1) Conduct internal research to develop, improve, or repair products, services, or technology;

(2) Effect a product recall;

(3) Identify and repair technical errors that impair existing or intended functionality; or

(4) Perform internal operations that:

(A) Are reasonably aligned with the expectations of the consumer;

(B) Are reasonably anticipated based on the consumer's existing relationship with the controller; or

(C) Are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) A controller or processor that processes personal data under an exemption in this subchapter bears the burden of demonstrating that the processing of the personal data:

(1) Qualifies for the exemption; and

(2) Complies with the requirements of § 4-120-306, § 4-120-405; and § 4-120-106(b).

(d) The processing of personal data by an entity for the purposes described by this chapter does not solely make the entity a controller with

respect to the processing of the data.

(e) This chapter supersedes and preempts an ordinance, resolution, rule, or other regulation adopted by a political subdivision regarding the processing of personal data by a controller or processor.

(f) A controller or processor that complies with the verifiable parental consent requirements of the Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 et seq., as it existed on January 1, 2025, with respect to data collected online is considered to be in compliance with any requirement to obtain parental consent under this chapter.

4-120-107. Requirements for small businesses and nonprofit organizations.

(a) A person that is a small business as described by § 4-120-104(a)(3) or a nonprofit organized as described by § 4-120-104(b) shall not engage in the sale of personal data without receiving prior consent from the consumer.

(b) A person who violates this section is subject to the penalty under § 4-120-701 et seq.

Subchapter 2 — Consumer Rights

4-120-201. Consumer's personal data rights — Request to exercise rights.

(a)(1) A consumer is entitled to exercise the consumer rights under this subchapter at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to exercise.

(2) With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise the consumer rights on behalf of the child.

(b) A controller shall comply with an authenticated consumer request to exercise the right to:

(1) Confirm whether a controller is processing the consumer's personal data and to access the personal data;

(2) Correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

(3) Delete personal data provided by or obtained about the consumer;

(4) If the data is available in a digital format, obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; or

(5) Opt out of the processing of the personal data for the purpose of:

(A) Targeted advertising;

(B) The sale of personal data; or

(C) Profiling in furtherance of a solely automated decision that produces a legal or similarly significant effect concerning the consumer.

4-120-202. Waiver or limitation of consumer rights prohibited.

A provision of a contract or agreement that waives or limits a consumer right described by §§ 4-120-201, 4-120-204, and 4-120-205 is contrary to public policy and is void.

4-120-203. Methods for submitting consumer requests.

(a)(1) A controller shall establish two (2) or more secure and reliable methods to enable consumers to submit a request to exercise their consumer rights under this chapter.

(2) The methods shall take into account:

(A) The ways in which consumers normally interact with the controller;

(B) The necessity for secure and reliable communications of any request under subdivision (a)(1) of this section; and

(C) The ability of the controller to authenticate the identity of the consumer making the request.

(b) A controller may not require a consumer to create a new account to exercise the consumer's rights under this chapter but may require a consumer to use an existing account.

(c) Except as provided by subsection (d) of this section, if the controller maintains a website, the controller shall provide a mechanism on

the website for consumers to submit requests for information required to be disclosed under this chapter.

(d) A controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal information is only required to provide an email address for the submission of requests described by subsection (c) of this section.

(e)(1) A consumer may designate:

(A) Another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data under § 4-120-201(b)(5)(A) and (B); or

(B) An authorized agent using a technology, including a link to a website, a browser setting or an extension, or a global setting on an electronic device, which allows the consumer to indicate the consumer's intent to opt out of the processing of the consumer's personal data.

(2) A controller shall comply with an opt-out request received from an authorized agent under this section if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

(3) A controller is not required to comply with an opt-out request received from an authorized agent under this subsection if:

(A) The authorized agent does not communicate the request to the controller in a clear and unambiguous *manner or comply with the controller's reasonable requirements for submitting requests*;

(B) The controller is not able to verify, with commercially reasonable effort, that the consumer is a resident of this state;

(C) The controller does not possess the ability to process the request; or

(D) The controller does not process similar or identical requests the controller receives from consumers for the purpose of complying with similar or identical laws or regulations of another state.

(f) A technology described under subsection (e) of this section:

(1) Shall not:

(A) Unfairly disadvantage another controller; or

(B) Make use of a default setting, but must require the consumer to consent and indicate the consumer's intent to opt out of any processing of a consumer's personal data; and

(2) Shall be consumer-friendly and easy to use by the average consumer.

4-120-204. Controller response to consumer request.

(a) Except as otherwise provided by this chapter, a controller shall comply with a request submitted by a consumer to exercise the consumer's rights under § 4-120-201 as provided by this section.

(b)(1) A controller shall respond to the consumer request without undue delay, which may not be later than the forty-fifth day after the date of receipt of the request.

(2) The controller may extend the response period once by an additional forty-five (45) days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial forty-five-day response period, together with the reason for the extension.

(c) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, which shall not be later than the forty-fifth day after the date of receipt of the request, of the justification for declining to take action and provide instructions on how to appeal the decision according to § 4-120-205.

(d)(1) A controller shall provide information in response to a consumer request free of charge, at least twice annually per consumer.

(2)(A) If a request from a consumer is manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request.

(B) The controller bears the burden of demonstrating for purposes of this subsection that a request is manifestly unfounded, excessive, or repetitive.

(e) If a controller is unable to authenticate the request using commercially reasonable efforts, the controller is not required to comply with a consumer request submitted under § 4-120-201 and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(f) A controller that has obtained personal data about a consumer from a source other than the consumer is considered in compliance with a consumer's request to delete the consumer's personal data under § 4-120-

201(b)(3) by:

(1) Retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted form the business's records and not using the retained data for any other purpose under this chapter; or

(2) Opting the consumer out of the processing of that personal data for any purpose other than a purpose that is exempt under the provisions of this chapter.

4-120-205. Appeal.

(a) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on the consumer's request under § 4-120-204(c).

(b) The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request under § 4-120-201.

(c) A controller shall inform the consumer in writing of any action taken or not taken in response to an appeal under this section not later than the sixtieth day after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.

(d) If the controller denies an appeal, the controller shall provide the consumer with the contact information of the Attorney General to submit a complaint.

Subchapter 3 — Controller Responsibilities

4-120-301. Notice of privacy practices.

(a) A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes:

(1) The categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller;

(2) The purpose for processing personal data;

(3) How consumers may exercise their consumer rights under § 4-120-201 et seq., including the process by which a consumer may appeal a controller's decision with regard to the consumer's request;

(4) If applicable, the categories of personal data that the

controller shares with third parties;

(5) If applicable, the categories of third parties with whom the controller shares personal data; and

(6) A description of the methods required under § 4-120-201 through which consumers can submit requests to exercise their consumer rights under this chapter.

(b)(1) If a controller engages in the sale of personal data that is sensitive data, the controller shall include the following notice: "NOTICE: We may sell your sensitive personal data.".

(2) The notice required under subdivision (b)(1) of this section shall be posted in the same location and in the same manner as the privacy notice described by subsection (a) of this section.

(c)(1) If a controller engages in the sale of personal data that is biometric data, the controller shall include the following notice: “NOTICE: We may sell your biometric personal data.”.

(2) The notice required under subdivision (c)(1) of this section shall be posted in the same location and in the same manner as the privacy notice described by subsection (a) of this section.

(d)(1) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the sale or *processing.*

(2) The controller shall provide the manner in which a consumer may exercise the right to opt out of the sale or process under subdivision (d)(1) of this section.

4-120-302. Lawful basis of processing.

(a) A person described under § 4-120-104 shall not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer.

(b) A person described under § 4-120-104 shall not otherwise process the personal information of a resident of this state without:

(1) The consent of the individual consumer;

(2) A contract that requires the processing of personal data;

(3) A legal obligation to process the personal data; or

(4) An overriding necessity to process the personal data of a person for the limited purpose of protecting the person’s vital interests.

(c) A person that is not a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as it existed on January 1, 2025, shall not collect or share any consumer health data except:

(1) With consent from the consumer for cash collection for a specified purpose; or

(2) To the extent necessary to provide a product or service that the consumer to whom the consumer health data relates has requested from the person.

(d) Consent required under subsection (c) of this section shall be obtained before the collection or sharing, as applicable, of any consumer health data, and the request for consent shall clearly and conspicuously disclose:

(1) The categories of consumer health data collected or shared;

(2) The purpose of the collection or sharing of the consumer health data, including the specific ways in which it will be used;

(3) The categories of entities with whom the consumer health data is shared; and

(4) How the consumer can withdraw consent from future collection or sharing of the consumer's health data.

(e) A controller shall not process the sensitive data of a consumer without obtaining the consumer's consent or, in the case of processing the sensitive data of a known child, without processing that data according to the Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 et seq., as it existed on January 1, 2025.

4-120-303. Dark patterns.

(a) A controller that collects personal information via a website, mobile application, or similar technology shall not utilize dark patterns in its user interfaces.

(b) A lawful basis for processing personal data described under § 4-120-302 obtained by use of a dark pattern is void.

4-120-304. Data minimization.

(a) A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes

for which that personal data is processed, as disclosed to the consumer.

(b) A controller in possession of deidentified data shall:

(1) Take reasonable measures to ensure that the data cannot be associated with an individual;

(2) Publicly commit to maintaining and using deidentified data without attempting to reidentify the data; and

(3) Contractually obligate any recipient of the deidentified data to comply with this section.

(c) This section does not require a controller to:

(1) Reidentify deidentified data or pseudonymous data;

(2) Maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data; or

(3) Comply with an authenticated consumer rights request under § 4-120-201, if the controller:

(A) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

(B) Does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same consumer; and

(C) Does not sell the personal data to a third party or otherwise voluntarily disclose the personal data to a third party other than a processor, except as otherwise permitted by this section.

(d) A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breach of the contractual commitments.

(e) This section shall not be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out under § 4-120-201 or the offer is related to a consumer's voluntary participation in a bona

fide loyalty, rewards, premium features, discounts, or club card program.

4-120-305. Data security.

A controller, for purposes of protecting the confidentiality, integrity, and accessibility of personal data, shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue.

4-120-306. Purpose limitation.

Personal data processed by a controller under this chapter:

(1) Shall not be processed for any purpose other than a purpose listed in this chapter unless otherwise allowed by this chapter;

(2) May be processed to the extent that the processing of data is:

(A) Reasonably necessary and proportionate to the purposes listed in this chapter; and

(B) Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this chapter; and

(3) Except as otherwise provided by this subchapter, a controller shall not process personal data for a purpose that is neither reasonably necessary to nor compatible with the purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

4-120-307. Data protection assessments.

(a) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

(1) The processing of personal data for purposes of targeted advertising;

(2) The sale of personal data;

(3) The processing of personal data for purposes of profiling if the profiling presents a reasonably foreseeable risk of:

(A) Unfair or deceptive treatment of or unlawful disparate impact on consumers;

(B) Financial, physical, or reputational injury to consumers;

(C) A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or

(D) Other substantial injury to consumers;

(4) The processing of sensitive data; and

(5) Any processing activities involving personal data that present a heightened risk of harm to consumers.

(b) A data protection assessment conducted under subsection (a) of this section shall:

(1) Identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with that processing as mitigated by safeguards that can be employed by the controller to reduce the risks; and

(2) Factor into the assessment:

(A) The use of deidentified data;

(B) The reasonable expectations of consumers;

(C) The context of the processing; and

(D) The relationship between the controller and the consumer whose personal data will be processed.

(c) A controller shall make a data protection assessment requested under § 4-120-701 et seq. available to the Attorney General under an Attorney General's subpoena under § 25-16-705.

(d)(1) A data protection assessment is confidential and exempt from public inspection and copying under the Freedom of Information Act of 1967, § 25-19-101 et seq.

(2) Disclosure of a data protection assessment in compliance with a request from the Attorney General does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(e) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(f) A data protection assessment conducted by a controller for the purpose of compliance with other laws or regulations may constitute

compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.

4-120-308. Pseudonymous data.

The consumer rights under § 4-120-201 and controller duties under this subchapter do not apply to pseudonymous data in cases in which the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

4-120-309. Miscellaneous prohibitions.

A controller shall not:

(1) Process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers; or

(2) Discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

Subchapter 4 — Processor Responsibilities

4-120-401. Compliance with contractual obligations.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting or complying with the controller's duties or requirements under this chapter, including without limitation:

(1) Assisting the controller in responding to consumer rights requests submitted under § 4-120-201 by using appropriate technical and organizational measures, as reasonably practicable, taking into account the nature of processing and the information available to the processor;

(2) Assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor's system, taking into account the nature of processing and the information available to the processor; and

(3) Providing necessary information to enable the controller to conduct and document data protection assessments under *§ 4-120-307*.

(b)(1) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller.

(2) The contract shall include:

(A) Clear instructions for processing data;

(B) The nature and purpose of processing;

(C) The type of data subject to processing;

(D) The duration of processing;

(E) The rights and obligations of both parties; and

(F) A requirement that the processor shall:

(i) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(ii) At the controller's direction, delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law;

(iii) Make available to the controller, on reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with the requirements of this chapter;

(iv) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; and

(v) Engage a subcontractor under a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data.

(c)(1) Notwithstanding the requirement described by subdivision (b)(2)(F) of this section, a processor, in the alternative, may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the requirements under this chapter using an appropriate and accepted control standard or framework and assessment procedure.

(2) The processor shall provide a report of the assessment to the controller on request.

(d) This section does not relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship as described by this chapter.

(e)(1) A determination of whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends on the context in which personal data is to be processed.

(2) A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains in the role of a processor.

Subchapter 5. [Reserved.]

Subchapter 6. [Reserved.]

Subchapter 7 — Enforcement

4-120-701. Attorney General.

The Attorney General has exclusive authority to enforce this chapter.

4-120-702. Procedures.

The Attorney General shall post on the Attorney General's website:

(1) Information relating to:

(A) The responsibilities of a controller under this chapter;

(B) The responsibilities of a processor under this *chapter; and*

(C) A consumer's rights under this chapter; and

(2) An online mechanism through which a consumer may submit a complaint under this chapter to the Attorney General.

4-120-703. Remedies.

(a)(1) If the Attorney General has reasonable cause to believe that a person has engaged in or is engaging in a violation of this chapter, the Attorney General may issue an Attorney General's subpoena.

(2) The procedures established for the issuance of an Attorney General's subpoena under § 25-16-705 apply to the same extent and manner to the issuance of an Attorney General's subpoena under this section.

(b)(1) The Attorney General may request, under an Attorney General's subpoena issued under subdivision (a)(1) of this section, that a person governed by this chapter disclose to any data protection assessment that is

relevant to an investigation conducted by the Attorney General.

(2) The Attorney General may evaluate the data protection *assessment for compliance with the requirements under § 4-120-307.*

(c) A violation of this chapter is an unfair and deceptive act or practice, as defined by the Deceptive Trade Practices Act, § 4-88-101 et seq.

(d) All remedies, penalties, and authority granted to the Attorney General under the Deceptive Trade Practices Act, § 4-88-101 et seq., shall be available to the Attorney General for the enforcement of this chapter.

4-120-704. Private right of action.

This chapter does not provide a basis for, or being subject to, a private right of action for a violation of this chapter or any other law.

Section 2. DO NOT CODIFY. Effective date.

(a) Sections 4-120-101 et seq. through sections § 4-120-401 et seq. are effective on January 1, 2026.

(b) To the extent § 4-120-701 et seq. applies to the enforcement of § 4-120-101 et seq. – § 4-120-401 et seq., it is effective on April 1, 2026.

/s/C. Penzo