INTERIM STUDY PROPOSAL 2023-003

State of Arkansas
94th General Assembly
Regular Session, 2023

A Bill

ANS/ANS
HOUSE BILL

By: Representative Dalby

Filed with: Arkansas Legislative Council
pursuant to A.C.A. §10-3-217.

For An Act To Be Entitled

AN ACT TO CREATE THE ARKANSAS CONSUMER DATA PROTECTION ACT; AND FOR OTHER PURPOSES.

Subtitle

TO CREATE THE ARKANSAS CONSUMER DATA PROTECTION ACT.

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

SECTION 1. Arkansas Code Title 4, Chapter 110, is amended to add an additional subchapter to read as follows:

Subchapter 2 — Arkansas Consumer Data Protection Act

4-110-201. Title.

This subchapter shall be known and may be cited as the "Arkansas Consumer Data Protection Act".

4-110-202. Definitions.

As used in this subchapter:

(1)(A) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity.

(B) As used this subchapter, "control" means:

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

(ii) Control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

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

(2) "Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his or her consumer rights in § 4-110-204, is the same consumer exercising 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, including without limitation:

(i) A fingerprint;

(ii) A voiceprint;

(iii) Eye retinas;

(iv) Irises; or

(v) Other unique biological patterns or characteristics that are used to identify a specific individual.

(B) "Biometric data" does not include a physical or digital photograph, a video or audio recording, or data generated from a physical or digital photograph or 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, Pub. L. No. 104-191, and related regulations under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January 1, 2023;

(4) "Business associate" means the same as defined under the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and related regulations under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January 1, 2023;

(5) "Child" means a person younger than thirteen (13) years of age;

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

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

(C) "Consent" does not include:

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

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

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

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

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

(9) "Covered entity" means the same as established by the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and related regulations under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January 1, 2023;

(10) "Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, healthcare services, or access to basic necessities, including food and water;

(11)(A) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to the person.

(B) A controller that possesses de-identified data shall comply with the requirements of § 4-110-208;

(12)(A) "Health record" means any written, printed or electronically recorded material maintained by a healthcare entity in the

course of providing health services to an individual concerning the individual and the services provided.

(B) "Health record" includes the substance of any communication made by an individual to a healthcare entity in confidence during or in connection with the provision of healthcare services or information otherwise acquired by the healthcare entity about an individual in confidence and in connection with the provision of healthcare services to the individual;

(13) "Healthcare provider" means a person who is licensed, certified, or otherwise authorized by the laws of this state to provide healthcare services;

(14) "Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly, in particular by reference to an identifier including a name, an identification number, precise geolocation data, or an online identifier;

(15) "Institution of higher education" means a public or private institution that provides postsecondary education or training to students that is academic, technical, trade-oriented, or in preparation for gaining employment in a recognized occupation;

(16) "Nonprofit organization" means an organization exempt from taxation under § 26 U.S.C. 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code;

(17) "Person" means:

(A) A natural person;

(B) A partnership;

(C) A corporation; or

(D) Any other business or legal entity;

(18)(A) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person.

(B) "Personal data" does not include de-identified data or publicly available information;

(19)(A) "Precise geolocation data" means information derived from technological resources, including without limitation global positioning system level latitude and longitude coordinates or other mechanisms that directly identify the specific location of a person 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 advanced utility metering infrastructure systems or equipment for use by a utility;

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

(21) "Processor" means a person that processes personal data on behalf of a controller;

(22) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements;

(23) "Protected health information" means the same as defined under the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and related regulations under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January 1, 2023;

(24) "Publicly available information" means information that is lawfully made available through federal, state, or local 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 the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience;

(25)(A) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the 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 behalf of the controller;

(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 the controller;

(iv) The disclosure of information that the consumer:

(a) Intentionally makes available to the general public via a channel of mass media; and

(b) Does 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, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets;

(26) "Sensitive data" means a category of personal data that includes:

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

(B) The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;

(C) The personal data collected from an identified or identifiable child; or

(D) Precise geolocation data;

(27)(A) "State agency" means an agency, institution, board, bureau, commission, council, or instrumentality of state government in the executive branch.

(B) "State agency" includes local officers of social services;

(28)(A) "Targeted advertising" means displaying advertisements to a consumer where the advertisement 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:

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

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

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

(iv) Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency; and

(29) "Third party" means a person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller.

4-110-203. Scope — Exemptions.

(a) This subchapter applies to persons that conduct business in this state or produce products or services that are targeted to residents of this state, and that:

(1) During a calendar year, control or process personal data of at least one hundred thousand (100,000) consumers; or

(2) Control or process personal data of at least twenty-five thousand (25,000) consumers and derive over fifty percent (50%) of gross revenue from the sale of personal data.

(b) This subchapter does not apply to:

(1) A body, authority, board, bureau, commission, district, or agency of the state or of any political subdivision of the state;

(2) A financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, Pub. L. No. 106-102;

(3) A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, 45 C.F.R. § 160 and § 164, as it existed on January 1, 2023, as established under the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and related regulations under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January 1, 2023, and the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5;

(4) A nonprofit organization; or

(5) An institution of higher education.

(c) The following information and data are exempt from this subchapter:

(1) Protected health information under the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, , and related regulations under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January 1, 2023;

(2) Health records for purposes of Title 20 of the Arkansas Code Annotated;

(3) Patient-identifying information for purposes of 42 U.S.C. § 290dd-2, as it existed on January 1, 2023;

(4) Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. § 46, as it existed on January 1, 2023;

(5) Identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(6) The protection of human subjects under 21 C.F.R. § 6, as it existed on January 1, 2023, 21 C.F.R. § 50, as it existed on January 1, 2023, and 21 C.F.R. § 56, as it existed on January 1, 2023, or personal data used or shared in research conducted according to the requirements stated in this subchapter, or other research conducted according to applicable law;

(7) 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, 2023;

(8) Patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005, Pub. L. No. 109-41;

(9) Information derived from any of the healthcare-related information listed in this subsection that is de-identified according to the requirements for de-identification under the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and related regulations under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January 1, 2023;

(10) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered

entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and related regulations under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January 1, 2023, or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2, as it existed on January 1, 2023;

(11) Information used only for public health activities and purposes as authorized by the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and related regulations under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January 1, 2023;

(12) The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, 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 a 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 et seq., as it existed on January 1, 2023;

(13) Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322;

(14) Personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g et seq., as it existed on January 1, 2023;

(15) 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, 2023; and

(16) Data processed or maintained:

(A) In the course of an individual applying to, 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;

(B) As the emergency contact information of an individual under this chapter used for emergency contact purposes; or

(C) That is necessary to retain to administer benefits for another individual relating to the individual under subdivision (c)(16)(A) of this section and used for the purposes of administering those benefits.

(d) Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act, Pub. L. No. 105-277, shall be deemed compliant with any obligation to obtain parental consent under this subchapter.

4-110-204. Personal data rights — Consumers.

(a)(1) A consumer may invoke the consumer rights authorized under this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke.

(2) A parent or legal guardian of an identified or identifiable child may invoke the consumer rights on behalf of the child regarding processing personal data belonging to the identified or identifiable child.

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

(A) To confirm whether or not a controller is processing the consumer's personal data and to access the personal data;

(B) To 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;

(C) To delete personal data maintained about the consumer;

(D) To 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, where the processing is carried out by automated means; and

(E) To opt out of the processing of the personal data for purposes of:

(i) Targeted advertising;

(ii) The sale of personal data; or

(iii) Profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.

(b) Except as otherwise provided in this subchapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized under subsection (a) of this section as follows:

(1) A controller shall respond to the consumer without undue delay, but in all cases within forty-five (45) days of receipt of the request submitted under the methods described in subsection (a) of this section;

(2) The response period may be extended once by forty-five (45) additional 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 any extension within the initial forty-five-day response period, together with the reason for the extension;

(3) If a controller declines to take action regarding the consumer's request, then the controller shall inform the consumer without undue delay, but in all cases and at the latest within forty-five (45) days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision under subsection (c) of this section;

(4)(A) Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer.

(B) If requests from a consumer are manifestly unfounded, excessive, or repetitive, then the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request.

(C) The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request;

(5) If a controller is unable to authenticate the request using commercially reasonable efforts, then the controller shall not be required to comply with a request to initiate an action under subsection (a) of this section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request; and

(6) A controller that has obtained personal data about a consumer from a source other than the consumer is considered to comply with a request by the consumer under subdivision (a)(3)(C) of this section to delete the consumer's personal data if the controller:

(A) Retains:

(i) A record of the consumer's request for deletion; and

(ii) The minimum data necessary to ensure that the consumer's personal data remains deleted from the controller's records; and

(B) Does not use the data retained under subdivision (b)(6)(A)(ii) of this section.

(c)(1) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision under subdivision (b)(3) of this section.

(2) The appeal process shall be conspicuously displayed and made readily available and similar to the process for submitting requests to initiate action under subsection (a) of this section.

(3)(A) Within sixty (60) days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

(B) If the appeal is denied, then the controller shall provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

4-110-205. Data controller responsibilities — Transparency.

(a) A controller shall:

(1) Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer; and

(2)(A) Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.

(B) The data security practices under subdivision (a)(2)(A) of this section shall be appropriate to the volume and nature of the personal data at issue.

(b) Except as otherwise provided in this subchapter, a controller shall not:

(1) Process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

(2) Process personal data in violation of state and federal laws that prohibit unlawful discrimination against a consumer;

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

(B) However, this subdivision (b)(3)(A) 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 his or her right to opt out under § 4-110-204 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and

(4) Process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning an identified or identifiable child, without processing the data according to the Children's Online Privacy Protection Act, Pub. L. No. 105-277.

(c) Any provision of a contract or agreement of any kind that purports to waive or limit in any way consumer rights under § 4-110-204 is contrary to public policy, void, and unenforceable.

(d) A controller shall provide a consumer with a reasonably accessible, clear, and meaningful privacy notice that includes:

(1) The categories of personal data processed by the controller;

(2) The purposes of processing personal data;

(3) Directions on how a consumer may exercise their consumer rights under § 4-110-204, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) The categories of personal data that the controller shares with third parties, if any; and

(5) The categories of third parties, if any, with whom the controller shares personal data.

(e) If a controller sells personal data to third parties or processes personal data for targeted advertising, then the controller shall clearly and conspicuously disclose the processing, as well as the manner in which a consumer may exercise the right to opt out of the processing.

(f)(1) A controller shall establish, and shall conspicuously describe in a privacy notice, one (1) or more secure and reliable means for a consumer to submit a request to exercise his or her consumer rights under this subchapter.

(2) The means under subdivision (f)(1) of this section shall take into account the:

(A) Ways in which a consumer normally interacts with the controller;

(B) Need for secure and reliable communication of the requests; and

(C)(i) Ability of the controller to authenticate the identity of the consumer making the request.

(ii) Controllers shall not require a consumer to create a new account in order to exercise consumer rights under § 4-110-204 but may require a consumer to use an existing account.

4-110-206. Responsibility according to role — Controller and processor.

(a)(1) A processor shall:

(A) Adhere to the instructions of a controller; and

(B) Assist the controller in meeting its obligations under this subchapter.

(2) The assistance required under subdivision (a)(1) of this section shall include without limitation, taking into account the nature of processing and the information available to the processor, by:

(A) Appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests under § 4-110-204;

(B) Assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the

processor under the Personal Information Protection Act, § 4-110-101 et seq., or this subchapter, in order to meet the controller's obligations; and

(C) Providing necessary information to enable the controller to conduct and document data protection assessments under § 4-110-207.

(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:

(A) Be binding and contain clearly stated instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties; and

(B) Include requirements 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 at the end of the provision of services, unless retention of the personal data is required by law;

(iii) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this subchapter;

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

(b) Alternatively, the processor 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 obligations under this subchapter using an appropriate and accepted control standard or framework and assessment procedure for the assessments.

(c) The processor shall provide a report of the assessment to the controller upon request; and

(v) Engage any subcontractor under a written contract according to subsection (c) of this section that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(c) Nothing in this section relieves a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this subchapter.

(d)(1) Determining 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 upon 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 a processor.

4-110-207. 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, where profiling presents a reasonably foreseeable risk of:

(A) Unfair or deceptive treatment of, or unlawful disparate impact on, a consumer;

(B) Financial, physical, or reputational injury to a consumer;

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

(D) Other substantial injury to a consumer;

(4) The processing of sensitive data; and

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

(b)(1) Data protection assessments conducted under subsection (a) of this section shall identify and weigh the benefits that may flow, directly and indirectly, 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 the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks.

(2) The use of de-identified data and the reasonable expectations of a consumer, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

(3)(A) The Attorney General may request, under a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General.

(B) The Attorney General may evaluate the data protection assessment for compliance with the responsibilities stated in § 4-110-205.

(C)(i) Data protection assessments shall be confidential and exempt from public inspection and copying under the Freedom of Information Act of 1967, § 25-19-101 et seq.

(ii) The disclosure of a data protection assessment following a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

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

(5) Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

(6) Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2024, and are not retroactive.

4-110-208. Processing de-identified data — Exemptions.

(a) A controller in possession of de-identified data shall:

(1) Take reasonable measures to ensure that the data cannot be associated with a natural person;

(2) Publicly commit to maintaining and using de-identified data without attempting to use the data to reidentify the data; and

(3) Contractually obligate any recipients of the de-identified data to comply with all provisions of this subchapter.

(b) This subchapter does not:

(1) Require a controller or processor to reidentify de-identified data;

(2) Maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data; or

(3) Require a controller or processor to comply with an authenticated consumer rights request, under § 4-110-204, if all of the following are true:

(A) The controller 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) The controller 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) The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(c) A controller that discloses de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

4-110-209. Limitations.

(a) This subchapter does not restrict a controller's or processor's ability to:

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

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

(3) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

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

(5) Provide a product or service specifically requested by a consumer, 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;

(6) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

(7) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any action under this subdivision (a)(7);

(8) 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 a similar independent oversight entity that determines:

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

(B) The expected benefits of the research outweigh the privacy risks; and

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

(9) Assist another controller, processor, or third party with any of the obligations under this subsection.

(b) The obligations imposed on controllers or processors under this chapter shall 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) Effectuate a product recall;

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

(4) Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, 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) The obligations imposed on controllers or processors under this subchapter shall not apply where compliance by the controller or processor with this subchapter would violate an evidentiary privilege under the laws of this state.

(d) This subchapter does not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(e)(1) A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this subchapter, is not in violation of this subchapter if the third-party controller or processor that receives and processes the personal data is in violation of this subchapter, if, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(2) A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this subchapter is likewise not in violation of this subchapter for the transgressions of the controller or processor from which it receives the personal data.

(f) This subchapter does not mean that an obligation is imposed on controllers and processors that adversely affects the rights or freedoms of any persons, including exercising the right of free speech under the First Amendment to the United States Constitution, or that it applies to the

processing of personal data by a person in the course of a purely personal or household activity.

(g)(1) Personal data processed by a controller under this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this subchapter.

(2) Personal data processed by a controller under this section may be processed to the extent that the processing is:

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

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

(3) Personal data collected, used, or retained under subsection (c) of this section shall, where applicable, take into account the nature and purpose or purposes of the collection, use, or retention.

(4) The data shall be 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 a consumer relating to the collection, use, or retention of personal data.

(5) If a controller processes personal data under an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in subsection (g) of this section.

(6) Processing personal data for the purposes expressly identified in subsection (a) of this section shall not solely make an entity a controller with respect to the processing.

4-110-210. Investigative authority.

If the Attorney General has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this subchapter, then the Attorney General may issue a civil investigative demand.

4-110-211. Enforcement — Civil penalty — Expenses.

(a) The Attorney General has exclusive authority to enforce the provisions of this subchapter.

(b)(1) Before initiating any action under this chapter, the Attorney General shall provide a controller or processor thirty (30) days' written notice identifying the specific provisions of this subchapter that the Attorney General alleges have been or are being violated.

(2) If within the thirty-day period under subdivision (b)(1) of this section, the controller or processor cures the identified violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations occur, no action shall be initiated against the controller or processor.

(c)(1) If a controller or processor continues to violate this subchapter following the thirty-day cure period in subsection (b) of this section or breaches an express written statement provided by the Attorney General under subsection (b) of this section, the Attorney General may initiate an action in the name of this state.

(2) The Attorney General may seek:

(A) An injunction to restrain any violations of this subchapter; and

(B) Civil penalties of up to seven thousand five hundred dollars ($7,500) for each violation under this subchapter.

(d) The Attorney General may recover reasonable expenses incurred in investigating and preparing for the case, including attorney's fees, in any action initiated under this subchapter.

(e) This subchapter does not provide the basis for or is not subject to a private right of action for violations of this subchapter or under any other law.

SECTION 2. Arkansas Code Title 19, Chapter 5, Subchapter 11, is amended to add an additional section to read as follows:

19-5-1158. Arkansas Consumer Privacy Trust Fund.

(a) There is created on the books of the Treasurer of State, the Auditor of State, and the Chief Fiscal Officer of the State a trust fund to be known as the "Arkansas Consumer Privacy Trust Fund".

(b) The fund shall consist of:

(1) All moneys received under the Arkansas Consumer Data Protection Act, § 4-110-201 et seq., including civil penalties, expenses, and attorney's fees; and

(2) All interest and income derived through investment of the fund.

(c)(1) The moneys in the fund shall be administered by and disbursed at the direction of the Attorney General.

(2) Moneys shall not be appropriated from the fund for any purpose except for the use and benefit of the Attorney General for administering the Arkansas Consumer Data Protection Act, § 4-110-201 et seq.

(3) The assets of the fund may be invested and reinvested as the Attorney General may determine.

(4) For the purposes of investment, fund moneys invested and interest earned on fund moneys invested shall be administered as trust funds under the State Treasury Management Law, § 19-3-501 et seq.

(5) All moneys deposited into the fund shall not be subject to any deduction, tax, levy, or any other type of assessment.

Referred by Representative Dalby

Prepared by: ANS/ANS