

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:

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

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

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

8 (2) "Authenticate" means verifying through reasonable means that
9 the consumer, entitled to exercise his or her consumer rights in § 4-110-204,
10 is the same consumer exercising consumer rights with respect to the personal
11 data at issue;

12 (3)(A) "Biometric data" means data generated by automatic
13 measurements of an individual's biological characteristics, including without
14 limitation:

15 (i) A fingerprint;

16 (ii) A voiceprint;

17 (iii) Eye retinas;

18 (iv) Irises; or

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

21 (B) "Biometric data" does not include a physical or
22 digital photograph, a video or audio recording, or data generated from a
23 physical or digital photograph or video or audio recording, or information
24 collected, used, or stored for healthcare treatment, payment, or operations
25 under the Health Insurance Portability and Accountability Act of 1996, Pub.
26 L. No. 104-191, and related regulations under 45 C.F.R. § 160, as it existed
27 on January 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45
28 C.F.R. § 164, as it existed on January 1, 2023;

29 (4) "Business associate" means the same as defined under the
30 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-
31 191, and related regulations under 45 C.F.R. § 160, as it existed on January
32 1, 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. §
33 164, as it existed on January 1, 2023;

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

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

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

7 (C) "Consent" does not include:

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

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

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

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

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

19 (9) "Covered entity" means the same as established by the Health
20 Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191,
21 and related regulations under 45 C.F.R. § 160, as it existed on January 1,
22 2023, 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164,
23 as it existed on January 1, 2023;

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

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

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

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

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

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

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

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

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

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

23 (17) "Person" means:

24 (A) A natural person;

25 (B) A partnership;

26 (C) A corporation; or

27 (D) Any other business or legal entity;

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

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

32 (19)(A) "Precise geolocation data" means information derived
33 from technological resources, including without limitation global positioning
34 system level latitude and longitude coordinates or other mechanisms that
35 directly identify the specific location of a person with precision and
36 accuracy within a radius of one thousand seven hundred fifty feet (1,750').

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

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

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

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

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

20 (24) "Publicly available information" means information that is
21 lawfully made available through federal, state, or local government records
22 or information that a business has a reasonable basis to believe is lawfully
23 made available to the general public through widely distributed media by the
24 consumer, or by a person to whom the consumer has disclosed the information,
25 unless the consumer has restricted the information to a specific audience;

26 (25)(A) "Sale of personal data" means the exchange of personal
27 data for monetary or other valuable consideration by the controller to a
28 third party.

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

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

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

35 (iii) The disclosure or transfer of personal data to
36 an affiliate of the controller;

1 (iv) The disclosure of information that the
2 consumer:

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

5 (b) Does not restrict to a specific audience;
6 or

7 (v) The disclosure or transfer of personal data to a
8 third party as an asset that is part of a merger, acquisition, bankruptcy, or
9 other transaction in which the third party assumes control of all or part of
10 the controller's assets;

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

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

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

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

20 (D) Precise geolocation data;

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

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

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

31 (B) "Targeted advertising" does not include:

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

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

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

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

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

8
9 4-110-203. Scope – Exemptions.

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

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

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

18 (b) This subchapter does not apply to:

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

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

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

32 (4) A nonprofit organization; or

33 (5) An institution of higher education.

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

1 (1) Protected health information under the Health Insurance
2 Portability and Accountability Act of 1996, Pub. L. No. 104-191, , and
3 related regulations under 45 C.F.R. § 160, as it existed on January 1, 2023,
4 45 C.F.R. § 162, as it existed on January 1, 2023, and 45 C.F.R. § 164, as it
5 existed on January 1, 2023;

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

8 (3) Patient-identifying information for purposes of 42 U.S.C. §
9 290dd-2, as it existed on January 1, 2023;

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

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

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

22 (7) Information and documents created for purposes of the Health
23 Care Quality Improvement Act of 1986, 42 U.S.C. § 11101 et seq., as it
24 existed on January 1, 2023;

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

27 (9) Information derived from any of the healthcare-related
28 information listed in this subsection that is de-identified according to the
29 requirements for de-identification under the Health Insurance Portability and
30 Accountability Act of 1996, Pub. L. No. 104-191, and related regulations
31 under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as
32 it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January
33 1, 2023;

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

1 entity or business associate as defined by the Health Insurance Portability
2 and Accountability Act of 1996, Pub. L. No. 104-191, and related regulations
3 under 45 C.F.R. § 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as
4 it existed on January 1, 2023, and 45 C.F.R. § 164, as it existed on January
5 1, 2023, or a program or a qualified service organization as defined by 42
6 U.S.C. § 290dd-2, as it existed on January 1, 2023;

7 (11) Information used only for public health activities and
8 purposes as authorized by the Health Insurance Portability and Accountability
9 Act of 1996, Pub. L. No. 104-191, and related regulations under 45 C.F.R. §
10 160, as it existed on January 1, 2023, 45 C.F.R. § 162, as it existed on
11 January 1, 2023, and 45 C.F.R. § 164, as it existed on January 1, 2023;

12 (12) The collection, maintenance, disclosure, sale,
13 communication, or use of any personal information bearing on a consumer's
14 credit worthiness, credit standing, credit capacity, character, general
15 reputation, personal characteristics, or mode of living by a consumer
16 reporting agency or furnisher that provides information for use in a consumer
17 report, and by a user of a consumer report, but only to the extent that the
18 activity is regulated by and authorized under the Fair Credit Reporting Act,
19 15 U.S.C. § 1681 et seq., as it existed on January 1, 2023;

20 (13) Personal data collected, processed, sold, or disclosed in
21 compliance with the Driver's Privacy Protection Act of 1994, Pub. L. No. 103-
22 322;

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

25 (15) Personal data collected, processed, sold, or disclosed in
26 compliance with the Farm Credit Act of 1971, 12 U.S.C. § 2001 et seq., as it
27 existed on January 1, 2023; and

28 (16) Data processed or maintained:

29 (A) In the course of an individual applying to, employed
30 by, or acting as an agent or independent contractor of a controller,
31 processor, or third party, to the extent that the data is collected and used
32 within the context of that role;

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

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

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

8
9 4-110-204. Personal data rights – Consumers.

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

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

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

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

20 (B) To correct inaccuracies in the consumer’s personal
21 data, taking into account the nature of the personal data and the purposes of
22 the processing of the consumer’s personal data;

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

24 (D) To obtain a copy of the consumer’s personal data that
25 the consumer previously provided to the controller in a portable and, to the
26 extent technically feasible, readily usable format that allows the consumer
27 to transmit the data to another controller without hindrance, where the
28 processing is carried out by automated means; and

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

31 (i) Targeted advertising;

32 (ii) The sale of personal data; or

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

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

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

7 (2) The response period may be extended once by forty-five (45)
8 additional days when reasonably necessary, taking into account the complexity
9 and number of the consumer's requests, so long as the controller informs the
10 consumer of any extension within the initial forty-five-day response period,
11 together with the reason for the extension;

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

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

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

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

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

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

1 (A) Retains:

2 (i) A record of the consumer’s request for deletion;

3 and

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

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

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

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

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

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

23
24 4-110-205. Data controller responsibilities – Transparency.

25 (a) A controller shall:

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

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

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

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

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

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

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

11 (B) However, this subdivision (b)(3)(A) shall not be
12 construed to require a controller to provide a product or service that
13 requires the personal data of a consumer that the controller does not collect
14 or maintain or to prohibit a controller from offering a different price,
15 rate, level, quality, or selection of goods or services to a consumer,
16 including offering goods or services for no fee, if the consumer has
17 exercised his or her right to opt out under § 4-110-204 or the offer is
18 related to a consumer's voluntary participation in a bona fide loyalty,
19 rewards, premium features, discounts, or club card program; and

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

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

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

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

31 (2) The purposes of processing personal data;

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

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

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

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

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

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

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

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

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

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

22
23 4-110-206. Responsibility according to role – Controller and processor.

24 (a)(1) A processor shall:

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

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

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

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

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

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

3 (C) Providing necessary information to enable the
4 controller to conduct and document data protection assessments under § 4-110-
5 207.

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

9 (2) The contract shall:

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

14 (B) Include requirements that the processor shall:

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

17 (ii) At the controller's direction, delete or return
18 all personal data to the controller as requested at the end of the provision
19 of services, unless retention of the personal data is required by law;

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

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

26 (b) Alternatively, the processor may arrange
27 for a qualified and independent assessor to conduct an assessment of the
28 processor's policies and technical and organizational measures in support of
29 the obligations under this subchapter using an appropriate and accepted
30 control standard or framework and assessment procedure for the assessments.

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

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

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

4 (d)(1) Determining whether a person is acting as a controller or
5 processor with respect to a specific processing of data is a fact-based
6 determination that depends upon the context in which personal data is to be
7 processed.

8 (2) A processor that continues to adhere to a controller's
9 instructions with respect to a specific processing of personal data remains a
10 processor.

11
12 4-110-207. Data protection assessments.

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

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

18 (2) The sale of personal data;

19 (3) The processing of personal data for purposes of profiling,
20 where profiling presents a reasonably foreseeable risk of:

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

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

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

28 (D) Other substantial injury to a consumer;

29 (4) The processing of sensitive data; and

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

32 (b)(1) Data protection assessments conducted under subsection (a) of
33 this section shall identify and weigh the benefits that may flow, directly
34 and indirectly, from the processing to the controller, the consumer, other
35 stakeholders, and the public against the potential risks to the rights of the

1 consumer associated with the processing, as mitigated by safeguards that can
2 be employed by the controller to reduce the risks.

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

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

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

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

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

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

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

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

30
31 4-110-208. Processing de-identified data – Exemptions.

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

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

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

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

3 (b) This subchapter does not:

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

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

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

12 (A) The controller is not reasonably capable of
13 associating the request with the personal data or it would be unreasonably
14 burdensome for the controller to associate the request with the personal
15 data;

16 (B) The controller does not use the personal data to
17 recognize or respond to the specific consumer who is the subject of the
18 personal data, or associate the personal data with other personal data about
19 the same consumer; and

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

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

27
28 4-110-209. Limitations.

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

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

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

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

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

6 (5) Provide a product or service specifically requested by a
7 consumer, perform a contract to which the consumer is a party, including
8 fulfilling the terms of a written warranty, or take steps at the request of
9 the consumer before entering into a contract;

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

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

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

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

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

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

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

33 (b) The obligations imposed on controllers or processors under this
34 chapter shall not restrict a controller's or processor's ability to collect,
35 use, or retain data to:

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

3 (2) Effectuate a product recall;

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

6 (4) Perform internal operations that are reasonably aligned with
7 the expectations of the consumer or reasonably anticipated based on the
8 consumer's existing relationship with the controller, are otherwise
9 compatible with processing data in furtherance of the provision of a product
10 or service specifically requested by a consumer, or the performance of a
11 contract to which the consumer is a party.

12 (c) The obligations imposed on controllers or processors under this
13 subchapter shall not apply where compliance by the controller or processor
14 with this subchapter would violate an evidentiary privilege under the laws of
15 this state.

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

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

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

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

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

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

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

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

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

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

15 (4) The data shall be subject to reasonable administrative,
16 technical, and physical measures to protect the confidentiality, integrity,
17 and accessibility of the personal data and to reduce reasonably foreseeable
18 risks of harm to a consumer relating to the collection, use, or retention of
19 personal data.

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

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

27
28 4-110-210. Investigative authority.

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

33
34 4-110-211. Enforcement – Civil penalty – Expenses.

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

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

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

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

15 (2) The Attorney General may seek:

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

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

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

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

26
27 SECTION 2. Arkansas Code Title 19, Chapter 5, Subchapter 11, is
28 amended to add an additional section to read as follows:

29 19-5-1158. Arkansas Consumer Privacy Trust Fund.

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

33 (b) The fund shall consist of:

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

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

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

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

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

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

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

15
16
17 Referred by Representative Dalby

18 Prepared by: ANS/ANS

19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36