

STATE OF OKLAHOMA

1st Session of the 60th Legislature (2025)

SENATE BILL 546

By: Howard

AS INTRODUCED

An Act relating to data privacy; defining terms; establishing consumer rights for processing of certain data; requiring compliance with certain consumer requests; establishing procedures for response to certain consumer requests; requiring establishment of certain appeal process; prohibiting certain contractual provisions; requiring establishment of methods for submission of certain consumer requests; establishing duties of controller; prohibiting controller from taking certain actions; providing exceptions; requiring privacy notice; specifying required contents in privacy notice; requiring certain disclosures; establishing duties of processor; establishing requirements for certain contracts; authorizing use of independent assessor under certain circumstances; requiring data protection assessments under certain circumstances; establishing requirements for data protection assessments; requiring availability of data protection assessments to Attorney General upon request; providing for confidentiality of data protection assessments; specifying applicability of requirements for data protection assessments; requiring controller in possession of certain data to take certain actions; providing enforcement authority to the Attorney General; requiring posting of certain information on Attorney General website; requiring notice of certain action; requiring certain period to cure violations before bringing certain action; providing penalties for certain violations; authorizing award of certain fees and expenses; providing for applicability of provisions; providing exceptions to applicability of provisions; exempting certain information; providing for compliance under certain circumstances; construing provisions;

1 authorizing processing of personal data for certain
2 purposes; prohibiting violation of evidentiary
3 privileges; clarifying certain liability; limiting
4 authorized purposes for processing of certain data;
5 providing for codification; and providing an
6 effective date.

7 BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

8 SECTION 1. NEW LAW A new section of law to be codified
9 in the Oklahoma Statutes as Section 300 of Title 75A, unless there
10 is created a duplication in numbering, reads as follows:

11 As used in this act:

12 1. "Affiliate" means a legal entity that controls, is
13 controlled by, or is under common control with another legal entity
14 or shares common branding with another legal entity. For purposes
15 of this paragraph, "control" or "controlled" means the:

- 16 a. ownership of, or power to vote, more than fifty
17 percent (50%) of the outstanding shares of any class
18 of voting securities of a company,
- 19 b. control in any manner over the election of a majority
20 of the directors or of individuals exercising similar
21 functions, or
- 22 c. power to exercise controlling influence over the
23 management of a company;

24 2. "Authenticate" means to verify through reasonable means that
the consumer who is entitled to exercise the consumer's rights under

1 this act is the same consumer exercising such consumer rights with
2 respect to the personal data at issue;

3 3. "Biometric data" means data generated by automatic
4 measurements of an individual's biological characteristics that is
5 used to identify a specific individual. The term includes, but is
6 not limited to, a fingerprint, voiceprint, eye retina or iris, or
7 other unique biological pattern or characteristic. The term does
8 not include a physical or digital photograph, a video or audio
9 recording, or data generated from a physical or digital photograph
10 or a video or audio recording unless such data is generated to
11 identify a specific individual. The term does not include
12 information collected, used, or stored for health care treatment,
13 payment, or operations under the Health Insurance Portability and
14 Accountability Act of 1996, 42 U.S.C., Section 1320d et seq.;

15 4. "Business associate" has the meaning assigned to the term
16 under the Health Insurance Portability and Accountability Act of
17 1996, 42 U.S.C., Section 1320d et seq. or any regulation adopted
18 thereunder;

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

21 6. "Consent", when referring to a consumer, means a clear
22 affirmative act signifying a consumer's freely given, specific,
23 informed, and unambiguous agreement to process personal data
24 relating to the consumer. The term includes, but is not limited to,

1 a written statement, including a statement written by electronic
2 means, or any other unambiguous affirmative action. The term does
3 not include:

4 a. acceptance of a general or broad terms of use or
5 similar document that contains descriptions of
6 personal data processing along with other, unrelated
7 information,

8 b. hovering over, muting, pausing, or closing a given
9 piece of content, or

10 c. agreement obtained through the use of dark patterns;

11 7. "Consumer" means an individual who is a resident of this
12 state acting only in an individual or household context. The term
13 does not include an individual acting in a commercial or employment
14 context;

15 8. "Controller" means an individual or other person that, alone
16 or jointly with others, determines the purpose and means of
17 processing personal data;

18 9. "Covered entity" has the meaning assigned to the term under
19 the Health Insurance Portability and Accountability Act of 1996, 42
20 U.S.C., Section 1320d et seq. or any regulation adopted thereunder;

21 10. "Dark pattern" means a user interface designed or
22 manipulated with the effect of substantially subverting or impairing
23 user autonomy, decision-making, or choice, and includes any practice
24 the Federal Trade Commission refers to as a dark pattern;

1 11. "Decision that produces a legal or similarly significant
2 effect concerning a consumer" means a decision made by the
3 controller that results in the provision or denial by the controller
4 of:

- 5 a. financial and lending services,
- 6 b. housing, insurance, or health care services,
- 7 c. education enrollment,
- 8 d. employment opportunities,
- 9 e. criminal justice, or
- 10 f. access to basic necessities such as food and water;

11 12. "De-identified data" means data that cannot reasonably be
12 linked to an identified or identifiable individual or a device
13 linked to the individual;

14 13. "Health care provider" has the meaning assigned to the term
15 under the Health Insurance Portability and Accountability Act of
16 1996, 42 U.S.C., Section 1320d et seq.;

17 14. "Health record" means any written, printed, or
18 electronically recorded material maintained by a health care
19 provider in the course of providing health care services to an
20 individual that concerns the individual and the services provided.
21 The term includes:

- 22 a. the substance of any communication made by an
23 individual to a health care provider in confidence

1 during or in connection with the provision of health
2 care services, or

- 3 b. information otherwise acquired by the health care
4 provider about an individual in confidence and in
5 connection with health care services provided to the
6 individual;

7 15. "Identified or identifiable individual" means a consumer
8 who can be readily identified, directly or indirectly;

9 16. "Institution of higher education" means:

- 10 a. a public institution that is a member of The Oklahoma
11 State System of Higher Education or a technology
12 center school district, or
13 b. a private institution of higher education;

14 17. "Nonprofit organization" means:

- 15 a. a corporation organized under Title 18 of the Oklahoma
16 Statutes to the extent applicable to nonprofit
17 corporations,
18 b. an organization exempt from federal taxation under
19 Section 501(a), Internal Revenue Code of 1986, as
20 amended, by being listed as an exempt organization
21 under Section 501(c)(3), 501(c)(6), or 501(c)(12) of
22 that code,
23 c. a political organization,
24 d. an organization that is:

1 (1) exempt from federal taxation under Section
2 501(a), Internal Revenue Code of 1986, as
3 amended, by being listed as an exempt
4 organization under Section 501(c)(4) of that
5 code, and

6 (2) described by Section 363 of Title 36 of the
7 Oklahoma Statutes, or

8 e. a subsidiary or affiliate of an entity regulated under
9 Section 151 et seq. of Title 17 of the Oklahoma
10 Statutes;

11 18. "Personal data" means any information including sensitive
12 data that is linked or reasonably linkable to an identified or
13 identifiable individual. The term includes pseudonymous data when
14 the data is used by a controller or processor in conjunction with
15 additional information that reasonably links the data to an
16 identified or identifiable individual. The term does not include
17 de-identified data or publicly available information;

18 19. "Political organization" means a party, committee,
19 association, fund, or other organization, regardless of whether
20 incorporated, that is organized and operated primarily for the
21 purpose of influencing or attempting to influence:

22 a. the selection, nomination, election, or appointment of
23 an individual to a federal, state, or local public
24 office or an office in a political organization,

1 regardless of whether the individual is selected,
2 nominated, elected, or appointed, or
3 b. the election of a presidential/vice-presidential
4 elector, regardless of whether the elector is
5 selected, nominated, elected, or appointed;

6 20. "Precise geolocation data" means information derived from
7 technology, including global positioning system level latitude and
8 longitude coordinates or other mechanisms, that directly identifies
9 the specific location of an individual with precision and accuracy
10 within a radius of one thousand seven hundred fifty (1,750) feet.
11 The term does not include the content of communications or any data
12 generated by or connected to an advanced utility metering
13 infrastructure system or to equipment for use by a utility;

14 21. "Process" or "processing" means an operation or set of
15 operations performed, whether by manual or automated means, on
16 personal data or on sets of personal data, such as the collection,
17 use, storage, disclosure, analysis, deletion, or modification of
18 personal data;

19 22. "Processor" means a person who processes personal data on
20 behalf of a controller or a service provider under contract with the
21 processor;

22 23. "Profiling" means any form of solely automated processing
23 performed on personal data to evaluate, analyze, or predict personal
24 aspects related to an identified or identifiable individual's
25

1 economic situation, health, personal preferences, interests,
2 reliability, behavior, location, or movements;

3 24. "Protected health information" has the meaning assigned to
4 the term under the Health Insurance Portability and Accountability
5 Act of 1996, 42 U.S.C., Section 1320d et seq. or any regulation
6 adopted thereunder;

7 25. "Pseudonymous data" means personal data that cannot be
8 attributed to a specific individual without the use of additional
9 information, provided that the additional information is kept
10 separately and is subject to appropriate technical and
11 organizational measures to ensure that the personal data is not
12 attributed to an identified or identifiable individual;

13 26. "Publicly available information" means information that is
14 lawfully made available through government records, or information
15 that a business has a reasonable basis to believe is lawfully made
16 available to the general public through widely distributed media, by
17 a consumer, or by a person to whom a consumer has disclosed the
18 information, unless the consumer has restricted the information to a
19 specific audience;

20 27. "Sale of personal data" means the exchange of personal data
21 for monetary consideration by the controller to a third party. The
22 term does not include the:
23
24
25

- a. disclosure of personal data to a processor that processes the personal data on the controller's behalf,
- b. disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer,
- c. disclosure or transfer of personal data to an affiliate of the controller,
- d. disclosure of information or personal data that the consumer:
 - (1) (a) intentionally made available to the general public through a mass media channel, and
 - (b) did not restrict to a specific audience, or
 - (2) directs the controller to disclose or intentionally uses the controller to interact with a third party, or
- e. disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets;

28. "Sensitive data" means a category of personal data. The term includes:

- a. personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status,
- b. genetic or biometric data that is processed for the purpose of uniquely identifying an individual,
- c. personal data collected from a known child, or
- d. precise geolocation data;

29. "State agency" means a department, commission, board, office, council, authority, or other agency in the executive branch of state government that is created by the constitution or a statute of this state, including a public university system or public institution of higher education;

30. "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. The term does not include:

- a. an advertisement that is:
 - (1) based on activities within a controller's own websites or online applications,
 - (2) based on the context of a consumer's current search query, visit to a website, or online application, or

1 (3) directed to a consumer in response to the
2 consumer's request for information or feedback,
3 or

4 b. the processing of personal data solely for measuring
5 or reporting advertising performance, reach, or
6 frequency;

7 31. "Third party" means a person other than the consumer, the
8 controller, the processor, a service provider under contract with
9 the controller or processor, or an affiliate of the controller or
10 processor; and

11 32. "Trade secret" means information including a formula,
12 pattern, compilation, program, device, method, technique, or
13 process, that:

14 a. derives independent economic value, actual or
15 potential, from not being generally known to, and not
16 being readily ascertainable by proper means by, other
17 persons who can obtain economic value from its
18 disclosure or use, and

19 b. is the subject of efforts that are reasonable under
20 the circumstances to maintain its secrecy.

21 SECTION 2. NEW LAW A new section of law to be codified
22 in the Oklahoma Statutes as Section 301 of Title 75A, unless there
23 is created a duplication in numbering, reads as follows:
24

1 A. A consumer is entitled to exercise the consumer rights
2 authorized by this section at any time by submitting a request to a
3 controller specifying the consumer rights the consumer wishes to
4 exercise. With respect to the processing of personal data belonging
5 to a known child, a parent or legal guardian of the child may
6 exercise the consumer rights on behalf of the child.

7 B. A controller shall comply with an authenticated consumer
8 request to exercise the right to:

9 1. Confirm whether a controller is processing the consumer's
10 personal data and to access the personal data;

11 2. Correct inaccuracies in the consumer's personal data,
12 considering the nature of the personal data and the purposes of the
13 processing of the consumer's personal data;

14 3. Delete personal data provided by or obtained about the
15 consumer;

16 4. If the data is available in a digital format, obtain a copy
17 of the consumer's personal data that the consumer previously
18 provided to the controller in a portable and, to the extent
19 technically feasible, readily usable format that allows the consumer
20 to transmit the data to another controller without hindrance, where
21 the processing is carried out by automated means; or

22 5. Opt out of the processing of the personal data for purposes
23 of:

24 a. targeted advertising,

- b. the sale of personal data, or
- c. profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.

SECTION 3. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 302 of Title 75A, unless there is created a duplication in numbering, reads as follows:

A. Except as otherwise provided by this act, a controller shall comply with a request submitted by a consumer to exercise the consumer's rights pursuant to Section 2 of this act as provided by this section.

B. A controller shall respond to the consumer request no later than forty-five (45) days after the date of receipt of the request. The controller may extend the response period once by an additional forty-five (45) days when reasonably necessary, considering the complexity and number of the consumer's requests. The controller shall inform the consumer of an extension within the initial forty-five-day response period and of the reason for the extension.

C. If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer no later than the forty-five (45) days 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 in accordance with Section 4 of this act.

1 D. A controller shall provide information in response to a
2 consumer request free of charge, up to twice annually per consumer.
3 If a request from a consumer is manifestly unfounded, excessive, or
4 repetitive, the controller may charge the consumer a reasonable fee
5 to cover the administrative costs of complying with the request or
6 may decline to act on the request. The controller shall bear the
7 burden of demonstrating for purposes of this subsection that a
8 request is manifestly unfounded, excessive, or repetitive.

9 E. If a controller is unable to authenticate the request using
10 commercially reasonable efforts, the controller shall not be
11 required to comply with a consumer request submitted under Section 2
12 of this act and may request that the consumer provide additional
13 information reasonably necessary to authenticate the consumer and
14 the consumer's request.

15 F. A controller that has obtained personal data about a
16 consumer from a source other than the consumer shall be considered
17 to be in compliance with a consumer's request to delete that
18 personal data pursuant to paragraph 3 of subsection B of Section 2
19 of this act by:

20 1. Retaining a record of the deletion request and the minimum
21 data necessary for the purpose of ensuring the consumer's personal
22 data remains deleted from the business's records and not using the
23 retained data for any other purpose under this act; or
24

1 2. Opting the consumer out of the processing of that personal
2 data for any purpose other than a purpose that is exempt under this
3 act.

4 SECTION 4. NEW LAW A new section of law to be codified
5 in the Oklahoma Statutes as Section 303 of Title 75A, unless there
6 is created a duplication in numbering, reads as follows:

7 A. A controller shall establish a process for a consumer to
8 appeal the controller's refusal to take action on a request within a
9 reasonable period of time after the consumer's receipt of the
10 decision under subsection C of Section 3 of this act. The appeal
11 process shall be conspicuously available and similar to the process
12 for initiating action to exercise consumer rights by submitting a
13 request under Section 2 of this act.

14 B. A controller shall inform the consumer in writing of any
15 action taken or not taken in response to an appeal under this
16 section no later than sixty (60) days after the date of receipt of
17 the appeal including a written explanation of the reason or reasons
18 for the decision. If the controller denies an appeal, the
19 controller shall provide the consumer with the online mechanism
20 described by subsection B of Section 12 of this act through which
21 the consumer may contact the Attorney General to submit a complaint.

22 SECTION 5. NEW LAW A new section of law to be codified
23 in the Oklahoma Statutes as Section 304 of Title 75A, unless there
24 is created a duplication in numbering, reads as follows:

1 Any provision of a contract or agreement that waives or limits a
2 consumer right described by Section 2, 3, or 4 of this act shall be
3 deemed to be contrary to public policy and shall be void and
4 unenforceable.

5 SECTION 6. NEW LAW A new section of law to be codified
6 in the Oklahoma Statutes as Section 305 of Title 75A, unless there
7 is created a duplication in numbering, reads as follows:

8 A controller shall establish two or more secure and reliable
9 methods to enable consumers to submit a request to exercise their
10 consumer rights under this act. The methods shall consider:

11 1. The ways in which consumers normally interact with the
12 controller;

13 2. The necessity for secure and reliable communications of
14 those requests; and

15 3. The ability of the controller to authenticate the identity
16 of the consumer making the request.

17 B. A controller shall not require a consumer to create a new
18 account to exercise the consumer's rights under this act but may
19 require a consumer to use an existing account.

20 C. Except as provided by subsection D of this section, if the
21 controller maintains an Internet website, the controller shall
22 provide a mechanism on the website for consumers to submit requests
23 for information required to be disclosed under this act.
24

1 D. A controller that operates exclusively online and has a
2 direct relationship with a consumer from whom the controller
3 collects personal information shall only be required to provide an
4 electronic mail address for the submission of requests described by
5 subsection C of this section.

6 SECTION 7. NEW LAW A new section of law to be codified
7 in the Oklahoma Statutes as Section 306 of Title 75A, unless there
8 is created a duplication in numbering, reads as follows:

9 A. A controller shall:

10 1. Limit the collection of personal data to what is adequate,
11 relevant, and reasonably necessary in relation to the purposes for
12 which that personal data is processed, as disclosed to the consumer;
13 and

14 2. For purposes of protecting the confidentiality, integrity,
15 and accessibility of personal data, establish, implement, and
16 maintain reasonable administrative, technical, and physical data
17 security practices that are appropriate to the volume and nature of
18 the personal data at issue.

19 B. A controller shall not:

20 1. Except as otherwise provided by this act, process personal
21 data for a purpose that is neither reasonably necessary to nor
22 compatible with the disclosed purpose for which the personal data is
23 processed, as disclosed to the consumer, unless the controller
24 obtains the consumer's consent;

1 2. Process personal data in violation of state and federal laws
2 that prohibit unlawful discrimination against consumers;

3 3. Discriminate against a consumer for exercising any consumer
4 rights contained in this act, including by denying goods or
5 services, charging different prices or rates for goods or services,
6 or providing a different level of quality of goods or services to
7 the consumer; or

8 4. Process the sensitive data of a consumer without obtaining
9 the consumer's consent or, in the case of processing the sensitive
10 data of a known child, without processing that data in accordance
11 with the Children's Online Privacy Protection Act of 1998, 15
12 U.S.C., Section 6501 et seq.

13 C. Paragraph 3 of subsection B of this section shall not be
14 construed to require a controller to provide a product or service
15 that requires the personal data of a consumer that the controller
16 does not collect or maintain or to prohibit a controller from
17 offering a different price, rate, level, quality, or selection of
18 goods or services to a consumer, including offering goods or
19 services for no fee, if the consumer has exercised the consumer's
20 right to opt out under Section 2 of this act or the offer is related
21 to a consumer's voluntary participation in a bona fide loyalty,
22 rewards, premium features, discounts, or club card program.

1 SECTION 8. NEW LAW A new section of law to be codified
2 in the Oklahoma Statutes as Section 307 of Title 75A, unless there
3 is created a duplication in numbering, reads as follows:

4 A. A controller shall provide consumers with a reasonably
5 accessible and clear privacy notice that includes:

6 1. The categories of personal data processed by the controller,
7 including, if applicable, any sensitive data processed by the
8 controller;

9 2. The purpose for processing personal data;

10 3. How consumers may exercise their consumer rights under
11 Sections 2 through 6 of this act, including the process by which a
12 consumer may appeal a controller's decision with regard to the
13 consumer's request;

14 4. If applicable, the categories of personal data that the
15 controller shares with third parties; and

16 5. If applicable, the categories of third parties with whom the
17 controller shares personal data.

18 B. If a controller sells personal data to third parties or
19 processes personal data for targeted advertising, the controller
20 shall clearly and conspicuously disclose on the notice required by
21 subsection A of this section such process and the manner in which a
22 consumer may exercise the right to opt out of such process.

1 SECTION 9. NEW LAW A new section of law to be codified
2 in the Oklahoma Statutes as Section 308 of Title 75A, unless there
3 is created a duplication in numbering, reads as follows:

4 A. A processor shall adhere to the instructions of a controller
5 and shall assist the controller in meeting or complying with the
6 controller's duties or requirements under this act, including:

7 1. Taking into account the nature of processing and the
8 information available to the processor, assisting the controller in
9 responding to consumer rights requests submitted under Section 2 of
10 this act by using appropriate technical and organizational measures,
11 as reasonably practicable;

12 2. Taking into account the nature of processing and the
13 information available to the processor, assisting the controller
14 with regard to complying with the requirement relating to the
15 security of processing personal data and to the notification of a
16 breach of security of the processor's system under the Security
17 Breach Notification Act, Section 161 et seq. of Title 24 of the
18 Oklahoma Statutes; and

19 3. Providing necessary information to enable the controller to
20 conduct and document data protection assessments under Section 10 of
21 this act.

22 B. A contract between a controller and a processor shall govern
23 the processor's data processing procedures with respect to
24
25

processing performed on behalf of the controller. The contract shall include:

1. Clear instructions for processing data;
2. The nature and purpose of processing;
3. The type of data subject to processing;
4. The duration of processing;
5. The rights and obligations of both parties; and
6. A requirement that the processor shall:
 - a. ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data,
 - b. 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,
 - c. make available to the controller, upon reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with the requirements of this act,
 - d. allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, and
 - e. engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the

1 requirements of the processor with respect to the
2 personal data.

3 C. Notwithstanding the requirement described by subparagraph d
4 of paragraph 6 of subsection B of this section, a processor, in the
5 alternative, may arrange for a qualified and independent assessor to
6 conduct an assessment of the processor's policies and technical and
7 organizational measures in support of the requirements under this
8 act using an appropriate and accepted control standard or framework
9 and assessment procedure. The processor shall provide a report of
10 the assessment to the controller on request.

11 D. The provisions of this section shall not be construed to
12 relieve a controller or a processor from the liabilities imposed on
13 the controller or processor due to its role in the processing
14 relationship as described by this act.

15 E. A determination of whether a person is acting as a
16 controller or processor with respect to a specific processing of
17 data is a fact-based determination that depends on the context in
18 which personal data is to be processed. A processor that continues
19 to adhere to a controller's instructions with respect to a specific
20 processing of personal data remains in the role of a processor.

21 SECTION 10. NEW LAW A new section of law to be codified
22 in the Oklahoma Statutes as Section 309 of Title 75A, unless there
23 is created a duplication in numbering, reads as follows:
24
25

1 A. A controller shall conduct and document a data protection
2 assessment of each of the following processing activities involving
3 personal data:

4 1. The processing of personal data for purposes of targeted
5 advertising;

6 2. The sale of personal data;

7 3. The processing of personal data for purposes of profiling,
8 if the profiling presents a reasonably foreseeable risk of:

9 a. unfair or deceptive treatment of or unlawful disparate
10 impact on consumers,

11 b. financial, physical, or reputational injury to
12 consumers,

13 c. a physical or other intrusion on the solitude or
14 seclusion, or the private affairs or concerns, of
15 consumers, if the intrusion would be offensive to a
16 reasonable person, or

17 d. other substantial injury to consumers;

18 4. The processing of sensitive data; and

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

21 B. A data protection assessment conducted under subsection A of
22 this section shall:

23 1. Identify and weigh the direct or indirect benefits that may
24 flow from the processing to the controller, the consumer, other

1 stakeholders, and the public, against the potential risks to the
2 rights of the consumer associated with that processing, as mitigated
3 by safeguards that can be employed by the controller to reduce the
4 risks; and

5 2. Factor into the assessment the:

- 6 a. use of de-identified data,
- 7 b. reasonable expectations of consumers,
- 8 c. context of the processing, and
- 9 d. relationship between the controller and the consumer
10 whose personal data will be processed.

11 C. A controller shall make a data protection assessment
12 available to the Attorney General upon written request pursuant to a
13 civil investigation demand.

14 D. A data protection assessment shall be confidential and
15 exempt from public inspection and copying under the Oklahoma Open
16 Records Act, Section 24A.1 et seq. of Title 51 of the Oklahoma
17 Statutes. Disclosure of a data protection assessment in compliance
18 with a request from the Attorney General shall not constitute a
19 waiver of attorney-client privilege or work product protection with
20 respect to the assessment and any information contained in the
21 assessment.

22 E. A single data protection assessment may address a comparable
23 set of processing operations that include similar activities.

1 F. A data protection assessment conducted by a controller for
2 the purpose of compliance with other laws or regulations may
3 constitute compliance with the requirements of this section if the
4 assessment has a reasonably comparable scope and effect.

5 G. A data protection assessment as required by this section
6 shall apply to processing activities that commence on or after the
7 effective date of this act and shall not be retroactive.

8 SECTION 11. NEW LAW A new section of law to be codified
9 in the Oklahoma Statutes as Section 310 of Title 75A, unless there
10 is created a duplication in numbering, reads as follows:

11 A. A controller in possession of de-identified data shall:

12 1. Take reasonable measures to ensure that the data cannot be
13 associated with an individual;

14 2. Publicly commit to maintaining and using de-identified data
15 without attempting to reidentify the data; and

16 3. Contractually obligate any recipient of the de-identified
17 data to comply with the provisions of this act.

18 B. The provisions of this act shall not be construed to require
19 a controller or processor to:

20 1. Reidentify de-identified data or pseudonymous data;

21 2. Maintain data in identifiable form or obtain, retain, or
22 access any data or technology for the purpose of allowing the
23 controller or processor to associate a consumer request with
24 personal data; or
25

1 3. Comply with an authenticated consumer rights request under
2 Section 2 of this act, if the controller:

- 3 a. is not reasonably capable of associating the request
4 with the personal data or it would be unreasonably
5 burdensome for the controller to associate the request
6 with the personal data,
7 b. does not use the personal data to recognize or respond
8 to the specific consumer who is the subject of the
9 personal data or associate the personal data with
10 other personal data about the same specific consumer,
11 and
12 c. does not sell the personal data to any third party or
13 otherwise voluntarily disclose the personal data to
14 any third party other than a processor, except as
15 otherwise permitted by this section.

16 C. The consumer rights under paragraphs 1 through 4 of
17 subsection B of Section 2 of this act and controller duties under
18 Section 7 of this act shall not apply to pseudonymous data in cases
19 in which the controller is able to demonstrate any information
20 necessary to identify the consumer is kept separately and is subject
21 to effective technical and organizational controls that prevent the
22 controller from accessing the information.

23 D. A controller that discloses pseudonymous data or de-
24 identified data shall exercise reasonable oversight to monitor
25

1 compliance with any contractual commitments to which the
2 pseudonymous data or de-identified data is subject and shall take
3 appropriate steps to address any breach of the contractual
4 commitments.

5 SECTION 12. NEW LAW A new section of law to be codified
6 in the Oklahoma Statutes as Section 311 of Title 75A, unless there
7 is created a duplication in numbering, reads as follows:

8 A. The Attorney General has exclusive authority to enforce the
9 provisions of this act.

10 B. The Attorney General shall post on the Attorney General's
11 Internet website:

12 1. Information relating to:

13 a. the responsibilities of a controller under this act,

14 b. the responsibilities of a processor under this act,

15 and

16 c. a consumer's rights under this act; and

17 2. An online mechanism through which a consumer may submit a
18 complaint under this act to the Attorney General.

19 SECTION 13. NEW LAW A new section of law to be codified
20 in the Oklahoma Statutes as Section 312 of Title 75A, unless there
21 is created a duplication in numbering, reads as follows

22 Before bringing an action under Section 14 of this act, the
23 Attorney General shall notify the controller or processor in
24 writing, no later than thirty (30) days before bringing the action,

1 identifying the specific provisions of this act that the Attorney
2 General alleges have been or are being violated. The Attorney
3 General shall not bring an action against the controller or
4 processor if:

5 1. Within the thirty-day period, the controller or processor
6 cures the identified violation; and

7 2. The controller or processor provides the Attorney General a
8 written statement that the controller or processor:

9 a. cured the alleged violation,

10 b. provided supportive documentation to show how the
11 privacy violation was cured, and

12 c. that no further violations will occur.

13 SECTION 14. NEW LAW A new section of law to be codified
14 in the Oklahoma Statutes as Section 313 of Title 75A, unless there
15 is created a duplication in numbering, reads as follows:

16 A. A controller or processor who violates this act following
17 the cure period described by Section 13 of this act or who breaches
18 a written statement provided to the Attorney General under such
19 section shall be liable for a civil penalty in an amount not to
20 exceed Seven Thousand Five Hundred Dollars (\$7,500.00) for each
21 violation.

22 B. The Attorney General may bring an action to:

23 1. Recover a civil penalty under this section;

24 2. Restrain or enjoin the person from violating this act; or
25

1 3. Recover the civil penalty and seek injunctive relief.

2 C. The court may award reasonable attorney fees and other
3 expenses incurred in investigating and bringing an action under this
4 section.

5 D. Civil penalties collected in an action under this section
6 shall be deposited in the State Treasury to the credit of the
7 General Revenue Fund.

8 E. Nothing in this act shall be construed as providing a basis
9 for, or being subject to, a private right of action for a violation
10 of this act or any other provision of law.

11 SECTION 15. NEW LAW A new section of law to be codified
12 in the Oklahoma Statutes as Section 314 of Title 75A, unless there
13 is created a duplication in numbering, reads as follows:

14 A. The provisions of this act apply only to a controller or
15 processor who:

16 1. Conducts business in this state or produces a product or
17 service targeted to the residents of this state; and

18 2. During a calendar year, either:

19 a. controls or processes personal data of at least one
20 hundred thousand (100,000) consumers, or

21 b. controls or processes personal data of at least
22 twenty-five thousand (25,000) consumers and derives
23 over fifty percent (50%) of gross revenue from the
24 sale of personal data.

1 B. The provisions of this act shall not apply to:

2 1. A state agency or a political subdivision of this state, or
3 a service provider processing data on behalf of a state agency or
4 political subdivision of this state;

5 2. A financial institution or data subject to Title V of the
6 Gramm-Leach-Bliley Act, 15 U.S.C., Section 6801 et seq.;

7 3. A covered entity or business associate governed by the
8 privacy, security, and breach notification rules issued by the
9 United States Department of Health and Human Services, 45 C.F.R.,
10 Parts 160 and 164, established under the Health Insurance
11 Portability and Accountability Act of 1996, 42 U.S.C., Section 1320d
12 et seq., and the Health Information Technology for Economic and
13 Clinical Health Act, Division A of Title XIII and Division B of
14 Title IV of the American Recovery and Reinvestment Act of 2009, Pub.
15 L. No. 111-5;

16 4. A nonprofit organization;

17 5. An institution of higher education; or

18 6. The processing of personal data by a person in the course of
19 a purely personal or household activity.

20 SECTION 16. NEW LAW A new section of law to be codified
21 in the Oklahoma Statutes as Section 315 of Title 75A, unless there
22 is created a duplication in numbering, reads as follows:

23 The following information shall be exempt from this act:
24
25

1 1. Protected health information under the Health Insurance
2 Portability and Accountability Act of 1996, 42 U.S.C., Section 1320d
3 et seq.;

4 2. Health records;

5 3. Patient identifying information for purposes of 42 U.S.C.,
6 Section 290dd-2;

7 4. Identifiable private information:

8 a. for purposes of the federal policy for the protection
9 of human subjects under 45 C.F.R., Part 46,

10 b. collected as part of human subjects research under the
11 good clinical practice guidelines issued by the
12 International Council for Harmonisation of Technical
13 Requirements for Pharmaceuticals for Human Use (ICH)
14 or of the protection of human subjects under 21
15 C.F.R., Parts 50 and 56, or

16 c. that is personal data used or shared in research
17 conducted in accordance with the requirements set
18 forth in this act or other research conducted in
19 accordance with applicable law;

20 5. Information and documents created for purposes of the Health
21 Care Quality Improvement Act of 1986, 42 U.S.C., Section 11101 et
22 seq.;

1 6. Patient safety work product for purposes of the Patient
2 Safety and Quality Improvement Act of 2005, 42 U.S.C., Section 299b-
3 21 et seq.;

4 7. Information derived from any of the health care-related
5 information listed in this section that is de-identified in
6 accordance with the requirements for de-identification under the
7 Health Insurance Portability and Accountability Act of 1996, 42
8 U.S.C., Section 1320d et seq. or any regulation adopted thereunder;

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

17 9. Information that is included in a limited data set as
18 described by 45 C.F.R., Section 164.514(e), to the extent that the
19 information is used, disclosed, and maintained in the manner
20 specified by 45 C.F.R., Section 164.514(e);

21 10. Information collected or used only for public health
22 activities and purposes as authorized under the Health Insurance
23 Portability and Accountability Act of 1996, 42 U.S.C., Section 1320d
24 et seq.;

1 11. The collection, maintenance, disclosure, sale,
2 communication, or use of any personal information bearing on a
3 consumer's creditworthiness, credit standing, credit capacity,
4 character, general reputation, personal characteristics, or mode of
5 living by a consumer reporting agency or furnisher that provides
6 information for use in a consumer report, and by a user of a
7 consumer report, but only to the extent that the activity is
8 regulated by and authorized under the Fair Credit Reporting Act, 15
9 U.S.C., Section 1681 et seq.;

10 12. Personal data collected, processed, sold, or disclosed in
11 compliance with the Driver's Privacy Protection Act of 1994, 18
12 U.S.C., Section 2721 et seq.;

13 13. Personal data regulated by the Family Educational Rights
14 and Privacy Act of 1974, 20 U.S.C., Section 1232g;

15 14. Personal data collected, processed, sold, or disclosed in
16 compliance with the Farm Credit Act of 1971, 12 U.S.C., Section 2001
17 et seq.;

18 15. Data processed or maintained in the course of an individual
19 applying to, being employed by, or acting as an agent or independent
20 contractor of a controller, processor, or third party, to the extent
21 that the data is collected and used within the context of such role;

22 16. Data processed or maintained as the emergency contact
23 information of an individual under this act that is used for
24 emergency contact purposes; or
25

1 17. Data that is processed or maintained and is necessary to
2 retain to administer benefits for another individual that relates to
3 an individual described by paragraph 15 of this section and used for
4 the purposes of administering those benefits.

5 SECTION 17. NEW LAW A new section of law to be codified
6 in the Oklahoma Statutes as Section 316 of Title 75A, unless there
7 is created a duplication in numbering, reads as follows:

8 A controller or processor that complies with the verifiable
9 parental consent requirements of the Children's Online Privacy
10 Protection Act of 1998, 15 U.S.C., Section 6501 et seq., with
11 respect to data collected online shall be considered to be in
12 compliance with any requirement to obtain parental consent under
13 this act.

14 SECTION 18. NEW LAW A new section of law to be codified
15 in the Oklahoma Statutes as Section 317 of Title 75A, unless there
16 is created a duplication in numbering, reads as follows:

17 A. The provisions of this act shall not be construed to
18 restrict a controller's or processor's ability to:

19 1. Comply with federal, state, or local laws, rules, or
20 regulations;

21 2. Comply with a civil, criminal, or regulatory inquiry,
22 investigation, subpoena, or summons by federal, state, local, or
23 other governmental authorities;

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

5 4. Investigate, establish, exercise, prepare for, or defend
6 legal claims;

7 5. Provide a product or service specifically requested by a
8 consumer or the parent or guardian of a child, perform a contract to
9 which the consumer is a party, including fulfilling the terms of a
10 written warranty, or take steps at the request of the consumer
11 before entering into a contract;

12 6. Take immediate steps to protect an interest that is
13 essential for the life or physical safety of the consumer or of
14 another individual and in which the processing cannot be manifestly
15 based on another legal basis;

16 7. Prevent, detect, protect against, or respond to security
17 incidents, identity theft, fraud, harassment, malicious or deceptive
18 activities, or any illegal activity;

19 8. Preserve the integrity or security of systems or
20 investigate, report, or prosecute those responsible for breaches of
21 system security;

22 9. Engage in public or peer-reviewed scientific or statistical
23 research in the public interest that adheres to all other applicable
24 ethics and privacy laws and is approved, monitored, and governed by

1 an institutional review board or similar independent oversight
2 entity that determines:

- 3 a. if the deletion of the information is likely to
4 provide substantial benefits that do not exclusively
5 accrue to the controller,
- 6 b. whether the expected benefits of the research outweigh
7 the privacy risks, and
- 8 c. if the controller has implemented reasonable
9 safeguards to mitigate privacy risks associated with
10 research, including any risks associated with
11 reidentification; or

12 10. Assist another controller, processor, or third party with
13 any of the requirements under this subsection.

14 B. The provisions of this act shall not be construed:

15 1. To prevent a controller or processor from providing personal
16 data concerning a consumer to a person covered by an evidentiary
17 privilege under the laws of this state as part of a privileged
18 communication;

19 2. As imposing a requirement on controllers and processors that
20 adversely affects the rights or freedoms of any person, including
21 the right of free speech; or

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

SECTION 19. NEW LAW A new section of law to be codified

in the Oklahoma Statutes as Section 318 of Title 75A, unless there is created a duplication in numbering, reads as follows:

A. The requirements imposed on controllers and processors under this act 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. Effect a product recall;

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

4. Perform internal operations that are:

a. reasonably aligned with the expectations of the consumer,

b. reasonably anticipated based on the consumer's existing relationship with the controller, or

c. 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.

B. A requirement imposed on a controller or processor under this act shall not apply if compliance with the requirement by the

1 controller or processor, as applicable, would violate an evidentiary
2 privilege under the laws of this state.

3 C. The processing of personal data by an entity for the
4 purposes described in subsection A of this section shall not solely
5 make the entity a controller with respect to the processing of the
6 data.

7 SECTION 20. NEW LAW A new section of law to be codified
8 in the Oklahoma Statutes as Section 319 of Title 75A, unless there
9 is created a duplication in numbering, reads as follows:

10 A. A controller or processor that discloses personal data to a
11 third-party controller or processor, in compliance with the
12 requirements of this act, shall not be deemed to be in violation of
13 this act if the third-party controller or processor that receives
14 and processes that personal data is in violation of this act;
15 provided, that at the time of the data's disclosure, the disclosing
16 controller or processor did not have actual knowledge that the
17 recipient intended to commit a violation.

18 B. A third-party controller or processor receiving personal
19 data from a controller or processor in compliance with the
20 requirements of this act shall not be deemed to be in violation of
21 this act for any wrongdoing of the controller or processor from
22 which the third-party controller or processor receives the personal
23 data.

SECTION 21. NEW LAW A new section of law to be codified in the Oklahoma Statutes as Section 320 of Title 75A, unless there is created a duplication in numbering, reads as follows:

A. Personal data processed by a controller shall not be processed for any purpose other than a purpose listed in Section 18, 19, or 20 of this act unless otherwise allowed by this act.

Personal data processed by a controller under Section 18, 19, or 20 of this act may be processed to the extent that the processing of the data is:

1. Reasonably necessary and proportionate to the purposes listed in Section 18, 19, or 20 of this act; and

2. Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in Section 18, 19, or 20 of this act.

B. Personal data collected, used, or retained under subsection A of Section 19 of this act shall, where applicable, consider the nature and purpose of such collection, use, or retention. The personal data described by this subsection 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.

C. A controller that processes personal data under an exemption in Section 18, 19, or 20 of this act bears the burden of

1 demonstrating that the processing of the personal data qualifies for
2 the exemption and complies with the requirements of subsections A
3 and B of this section.

4 D. The processing of personal data by an entity for the
5 purposes described by Section 18 of this act does not solely make
6 the entity a controller with respect to the processing of the data.

7 SECTION 22. This act shall become effective January 1, 2026.

8
9 60-1-57 CN 1/13/2025 1:27:39 PM
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25