

1 ENGROSSED HOUSE AMENDMENTS

TO

2 ENGROSSED SENATE BILL NO. 546

By: Howard of the Senate

3 and

4 West (Josh) of the House

5

6

7 [data privacy - consumer rights - consumer requests
8 - appeal process - exceptions - privacy notice -
disclosures - contracts - data protection assessments
9 - action - penalties - fees and expenses -
evidentiary privileges - liability - codification -
effective date]

10

11

12 AUTHOR: Add the following House Coauthors: Archer, Pae, Provenzano,
and Waldron

13

14 AMENDMENT NO. 1. Strike the stricken title, enacting clause, and
entire bill and insert:

15

16

17 "An Act relating to data privacy; defining terms;
18 establishing consumer rights for processing of
certain data; requiring compliance with certain
19 consumer requests; establishing procedures for
response to certain consumer requests; requiring
20 establishment of certain appeal process; prohibiting
certain contractual provisions; requiring
21 establishment of methods for submission of certain
consumer requests; establishing duties of controller;
22 prohibiting controller from taking certain actions;
providing exceptions; requiring privacy notice;
23 specifying required contents in privacy notice;
requiring certain disclosures; establishing duties of
24 processor; establishing requirements for certain
contracts; authorizing use of independent assessor

1 under certain circumstances; requiring data
2 protection assessments under certain circumstances;
3 establishing requirements for data protection
4 assessments; requiring availability of data
5 protection assessments to Attorney General upon
6 request; providing for confidentiality of data
7 protection assessments; specifying applicability of
8 requirements for data protection assessments;
9 requiring controller in possession of certain data to
10 take certain actions; providing enforcement authority
11 to the Attorney General; requiring posting of certain
12 information on Attorney General website; requiring
13 notice of certain action; requiring certain period to
14 cure violations before bringing certain action;
15 providing penalties for certain violations;
16 authorizing award of certain fees and expenses;
17 providing for applicability of provisions; providing
18 exceptions to applicability of provisions; exempting
19 certain information; providing for compliance under
20 certain circumstances; providing construing
21 provisions; authorizing processing of personal data
22 for certain purposes; prohibiting violation of
23 evidentiary privileges; clarifying certain liability;
24 limiting authorized purposes for processing of
certain data; providing for codification; and
providing an effective date.

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

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

As used in this act:

1. "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. For purposes
of this paragraph, "control" or "controlled" means the:

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

2. "Authenticate" means to verify through reasonable means that the consumer who is entitled to exercise the consumer's rights under this act is the same consumer exercising such consumer rights with respect to the personal data at issue;

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

1 4. "Business associate" has the meaning assigned to the term
2 under the Health Insurance Portability and Accountability Act of
3 1996, 42 U.S.C., Section 1320d et seq. or any regulation adopted
4 thereunder;

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

7 6. "Children's Online Privacy Protection Act of 1998" means 15
8 U.S.C., Section 6501 et seq. and includes the regulations, rules,
9 guidance, and exemptions adopted pursuant to the act and any
10 subsequent amendments;

11 7. "Consent", when referring to a consumer, means a clear
12 affirmative act signifying a consumer's freely given, specific,
13 informed, and unambiguous agreement to process personal data
14 relating to the consumer. The term includes, but is not limited to,
15 a written statement, including a statement written by electronic
16 means, or any other unambiguous affirmative action. The term does
17 not include:

18 a. acceptance of a general or broad terms of use or
19 similar document that contains descriptions of
20 personal data processing along with other, unrelated
21 information,

22 b. hovering over, muting, pausing, or closing a given
23 piece of content, or

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

1 8. "Consumer" means an individual who is a resident of this
2 state acting only in an individual or household context. The term
3 does not include an individual acting in a commercial or employment
4 context;

5 9. "Controller" means an individual or other person that, alone
6 or jointly with others, determines the purpose and means of
7 processing personal data;

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

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

15 12. "Decision that produces a legal or similarly significant
16 effect concerning a consumer" means a decision made by the
17 controller that results in the provision or denial by the controller
18 of:

- 19 a. financial and lending services,
- 20 b. housing, insurance, or health care services,
- 21 c. education enrollment,
- 22 d. employment opportunities,
- 23 e. criminal justice, or
- 24 f. access to basic necessities such as food and water;

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

4 14. "Health care provider" has the meaning assigned to the term
5 under the Health Insurance Portability and Accountability Act of
6 1996, 42 U.S.C., Section 1320d et seq.;

7 15. "Health record" means any written, printed, or
8 electronically recorded material maintained by a health care
9 provider in the course of providing health care services to an
10 individual that concerns the individual and the services provided.

11 The term includes:

- 12 a. the substance of any communication made by an
13 individual to a health care provider in confidence
14 during or in connection with the provision of health
15 care services, or
- 16 b. information otherwise acquired by the health care
17 provider about an individual in confidence and in
18 connection with health care services provided to the
19 individual;

20 16. "Identified or identifiable individual" means a consumer
21 who can be readily identified, directly or indirectly;

22 17. "Institution of higher education" means:
23
24

- 1 a. a public institution that is a member of The Oklahoma
- 2 State System of Higher Education or a technology
- 3 center school district, or
- 4 b. a private institution of higher education;

5 18. "Nonprofit organization" means:

- 6 a. a corporation organized under Title 18 of the Oklahoma
- 7 Statutes to the extent applicable to nonprofit
- 8 corporations,
- 9 b. an organization exempt from federal taxation under
- 10 Section 501(a), Internal Revenue Code of 1986, as
- 11 amended, by being listed as an exempt organization
- 12 under Section 501(c) (3), 501(c) (6), or 501(c) (12) of
- 13 that code,
- 14 c. a political organization,
- 15 d. an organization that is:
 - 16 (1) exempt from federal taxation under Section
 - 17 501(a), Internal Revenue Code of 1986, as
 - 18 amended, by being listed as an exempt
 - 19 organization under Section 501(c) (4) of that
 - 20 code, and
 - 21 (2) described by Section 363 of Title 36 of the
 - 22 Oklahoma Statutes, or

1 e. a subsidiary or affiliate of an entity regulated under
2 Section 151 et seq. of Title 17 of the Oklahoma
3 Statutes;

4 19. "Personal data" means any information including sensitive
5 data that is linked or reasonably linkable to an identified or
6 identifiable individual. The term includes pseudonymous data when
7 the data is used by a controller or processor in conjunction with
8 additional information that reasonably links the data to an
9 identified or identifiable individual. The term does not include
10 de-identified data or publicly available information;

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

- 15 a. the selection, nomination, election, or appointment of
16 an individual to a federal, state, or local public
17 office or an office in a political organization,
18 regardless of whether the individual is selected,
19 nominated, elected, or appointed, or
20 b. the election of a presidential/vice-presidential
21 elector, regardless of whether the elector is
22 selected, nominated, elected, or appointed;

23 21. "Precise geolocation data" means information derived from
24 technology, including global positioning system level latitude and

1 longitude coordinates or other mechanisms, that directly identifies
2 the specific location of an individual with precision and accuracy
3 within a radius of one thousand seven hundred fifty (1,750) feet.
4 The term does not include the content of communications, nor does it
5 include any data generated by or connected to an advanced utility
6 metering infrastructure system or to equipment for use by a utility;

7 22. "Process" or "processing" means any operation or set of
8 operations performed, whether by manual or automated means, on
9 personal data or on sets of personal data, such as the collection,
10 use, storage, disclosure, analysis, deletion, or modification of
11 personal data;

12 23. "Processor" means a person who, or legal entity that,
13 processes personal data on behalf of a controller;

14 24. "Profiling" means any form of solely automated processing
15 performed on personal data to evaluate, analyze, or predict personal
16 aspects related to an identified or identifiable individual's
17 economic situation, health, personal preferences, interests,
18 reliability, behavior, location, or movements;

19 25. "Protected health information" has the meaning assigned to
20 the term under the Health Insurance Portability and Accountability
21 Act of 1996, 42 U.S.C., Section 1320d et seq. or any regulation
22 adopted thereunder;

23 26. "Pseudonymous data" means personal data that cannot be
24 attributed to a specific individual without the use of additional

1 information, provided that the additional information is kept
2 separately and is subject to appropriate technical and
3 organizational measures to ensure that the personal data is not
4 attributed to an identified or identifiable individual;

5 27. "Publicly available information" means information that is
6 lawfully made available through government records, or information
7 that a business has a reasonable basis to believe is lawfully made
8 available to the general public through widely distributed media, by
9 a consumer, or by a person to whom a consumer has disclosed the
10 information, unless the consumer has restricted the information to a
11 specific audience;

12 28. "Sale of personal data" means the exchange of personal data
13 for monetary consideration by the controller to a third party. The
14 term does not include the:

- 15 a. disclosure of personal data to a processor that
16 processes the personal data on the controller's
17 behalf,
- 18 b. disclosure of personal data to a third party for
19 purposes of providing a product or service requested
20 by the consumer,
- 21 c. disclosure or transfer of personal data to an
22 affiliate of the controller,
- 23 d. disclosure of information or personal data that the
24 consumer:

- 1 (1) (a) intentionally made available to the general
2 public through a mass media channel, and
3 (b) did not restrict to a specific audience, or
4 (2) directs the controller to disclose or
5 intentionally uses the controller to interact
6 with a third party, or
7 e. disclosure or transfer of personal data to a third
8 party as an asset that is part of a proposed or actual
9 merger, acquisition, bankruptcy, or other transaction
10 in which the third party assumes control of all or
11 part of the controller's assets;

12 29. "Sensitive data" means a category of personal data. The
13 term includes:

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

22 30. "State agency" means a department, commission, board,
23 office, council, authority, or other agency in the executive branch
24 of state government that is created by the constitution or a statute

1 of this state, including a public university system or public
2 institution of higher education;

3 31. "Targeted advertising" means displaying to a consumer an
4 advertisement that is selected based on personal data obtained from
5 that consumer's activities over time and across nonaffiliated
6 websites or online applications to predict the consumer's
7 preferences or interests. The term does not include:

8 a. an advertisement that is:

9 (1) based on activities within a controller's own
10 websites or online applications,

11 (2) based on the context of a consumer's current
12 search query, visit to a website, or online
13 application, or

14 (3) directed to a consumer in response to the
15 consumer's request for information or feedback,
16 or

17 b. the processing of personal data solely for measuring
18 or reporting advertising performance, reach, or
19 frequency;

20 32. "Third party" means a person other than the consumer, the
21 controller, the processor, or an affiliate of the controller or
22 processor; and
23
24

1 33. "Trade secret" means information including a formula,
2 pattern, compilation, program, device, method, technique, or
3 process, that:

4 a. derives independent economic value, actual or
5 potential, from not being generally known to, and not
6 being readily ascertainable by proper means by, other
7 persons who can obtain economic value from its
8 disclosure or use, and

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

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

14 A. A consumer is entitled to exercise the consumer rights
15 authorized by this section at any time by submitting a request to a
16 controller specifying the consumer rights the consumer wishes to
17 exercise. With respect to the processing of personal data belonging
18 to a known child, a parent or legal guardian of the child may
19 exercise the consumer rights on behalf of the child.

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

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

1 2. Correct inaccuracies in the consumer's personal data,
2 considering the nature of the personal data and the purposes of the
3 processing of the consumer's personal data;

4 3. Delete personal data provided by or obtained about the
5 consumer;

6 4. If the data is available in a digital format, obtain a copy
7 of the consumer's personal data that the consumer previously
8 provided to the controller in a portable and, to the extent
9 technically feasible, readily usable format that allows the consumer
10 to transmit the data to another controller without hindrance, where
11 the processing is carried out by automated means; or

12 5. Opt out of the processing of the personal data for purposes
13 of:

14 a. targeted advertising,

15 b. the sale of personal data, or

16 c. profiling in furtherance of a decision that produces a
17 legal or similarly significant effect concerning the
18 consumer.

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

22 A. Except as otherwise provided by this act, a controller shall
23 comply with a request submitted by a consumer to exercise the
24

1 consumer's rights pursuant to Section 2 of this act as provided by
2 this section.

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

10 C. If a controller declines to take action regarding the
11 consumer's request, the controller shall inform the consumer no
12 later than the forty-five (45) days after the date of receipt of the
13 request of the justification for declining to take action and
14 provide instructions on how to appeal the decision in accordance
15 with Section 4 of this act.

16 D. A controller shall provide information in response to a
17 consumer request free of charge, up to twice annually per consumer.
18 If a request from a consumer is manifestly unfounded, excessive, or
19 repetitive, the controller may charge the consumer a reasonable fee
20 to cover the administrative costs of complying with the request or
21 may decline to act on the request. The controller shall bear the
22 burden of demonstrating for purposes of this subsection that a
23 request is manifestly unfounded, excessive, or repetitive.

24

1 E. If a controller is unable to authenticate the request using
2 commercially reasonable efforts, the controller shall not be
3 required to comply with a consumer request submitted under Section 2
4 of this act and may request that the consumer provide additional
5 information reasonably necessary to authenticate the consumer and
6 the consumer's request.

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

12 1. Retaining a record of the deletion request and the minimum
13 data necessary for the purpose of ensuring the consumer's personal
14 data remains deleted from the business's records and not using the
15 retained data for any other purpose under this act; or

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

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

22 A. A controller shall establish a process for a consumer to
23 appeal the controller's refusal to take action on a request within a
24 reasonable period of time after the consumer's receipt of the

1 decision under subsection C of Section 3 of this act. The appeal
2 process shall be conspicuously available and similar to the process
3 for initiating action to exercise consumer rights by submitting a
4 request under Section 2 of this act.

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

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

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

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

23
24

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

4 1. The ways in which consumers normally interact with the
5 controller;

6 2. The necessity for secure and reliable communications of
7 those requests; and

8 3. The ability of the controller to authenticate the identity
9 of the consumer making the request.

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

13 C. Except as provided by subsection D of this section, if the
14 controller maintains an Internet website, the controller shall
15 provide a mechanism on the website for consumers to submit requests
16 for information required to be disclosed under this act.

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

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

1 A. A controller shall:

2 1. Limit the collection of personal data to what is adequate,
3 relevant, and reasonably necessary in relation to the purposes for
4 which that personal data is processed, as disclosed to the consumer;
5 and

6 2. For purposes of protecting the confidentiality, integrity,
7 and accessibility of personal data, establish, implement, and
8 maintain reasonable administrative, technical, and physical data
9 security practices that are appropriate to the volume and nature of
10 the personal data at issue.

11 B. A controller shall not:

12 1. Except as otherwise provided by this act, process personal
13 data for a purpose that is neither reasonably necessary to nor
14 compatible with the disclosed purpose for which the personal data is
15 processed, as disclosed to the consumer, unless the controller
16 obtains the consumer's consent;

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

19 3. Discriminate against a consumer for exercising any consumer
20 rights contained in this act, including by denying goods or
21 services, charging different prices or rates for goods or services,
22 or providing a different level of quality of goods or services to
23 the consumer; or

1 4. Process the sensitive data of a consumer without obtaining
2 the consumer's consent or, in the case of processing the sensitive
3 data of a known child, without processing that data in accordance
4 with the Children's Online Privacy Protection Act of 1998.

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

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

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

20 1. The categories of personal data processed by the controller,
21 including, if applicable, any sensitive data processed by the
22 controller;

23 2. The purpose for processing personal data;

24

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

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

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

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

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

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

20 1. Taking into account the nature of processing and the
21 information available to the processor, assisting the controller in
22 responding to consumer rights requests submitted under Section 2 of
23 this act by using appropriate technical and organizational measures,
24 as reasonably practicable;

1 2. Taking into account the nature of processing and the
2 information available to the processor, assisting the controller
3 with regard to complying with the requirement relating to the
4 security of processing personal data and to the notification of a
5 breach of security of the processor's system under the Security
6 Breach Notification Act, Section 161 et seq. of Title 24 of the
7 Oklahoma Statutes; and

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

11 B. A contract between a controller and a processor shall govern
12 the processor's data processing procedures with respect to
13 processing performed on behalf of the controller. The contract
14 shall include:

- 15 1. Clear instructions for processing data;
- 16 2. The nature and purpose of processing;
- 17 3. The type of data subject to processing;
- 18 4. The duration of processing;
- 19 5. The rights and obligations of both parties; and
- 20 6. A requirement that the processor shall:
 - 21 a. ensure that each person processing personal data is
22 subject to a duty of confidentiality with respect to
23 the data,

24

- 1 b. at the controller's direction, delete or return all
2 personal data to the controller as requested after the
3 provision of the service is completed, unless
4 retention of the personal data is required by law,
5 c. make available to the controller, upon reasonable
6 request, all information in the processor's possession
7 necessary to demonstrate the processor's compliance
8 with the requirements of this act,
9 d. allow, and cooperate with, reasonable assessments by
10 the controller or the controller's designated
11 assessor, and
12 e. engage any subcontractor pursuant to a written
13 contract that requires the subcontractor to meet the
14 requirements of the processor with respect to the
15 personal data.

16 C. Notwithstanding the requirement described by subparagraph d
17 of paragraph 6 of subsection B of this section, a processor, in the
18 alternative, may arrange for a qualified and independent assessor to
19 conduct an assessment of the processor's policies and technical and
20 organizational measures in support of the requirements under this
21 act using an appropriate and accepted control standard or framework
22 and assessment procedure. The processor shall provide a report of
23 the assessment to the controller on request.

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

5 E. A determination of whether a person is acting as a
6 controller or processor with respect to a specific processing of
7 data is a fact-based determination that depends on the context in
8 which personal data is to be processed. A processor that continues
9 to adhere to a controller's instructions with respect to a specific
10 processing of personal data remains in the role of a processor.

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

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

17 1. The processing of personal data for purposes of targeted
18 advertising;

19 2. The sale of personal data;

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

22 a. unfair or deceptive treatment of or unlawful disparate
23 impact on consumers,
24

- b. financial, physical, or reputational injury to consumers,
- c. a physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person, or
- d. other substantial injury to consumers;

4. The processing of sensitive data; and

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

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

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

2. Factor into the assessment the:

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

1 C. A controller shall make a data protection assessment
2 available to the Attorney General upon written request pursuant to a
3 civil investigation demand.

4 D. A data protection assessment shall be confidential and
5 exempt from public inspection and copying under the Oklahoma Open
6 Records Act, Section 24A.1 et seq. of Title 51 of the Oklahoma
7 Statutes. Disclosure of a data protection assessment in compliance
8 with a request from the Attorney General shall not constitute a
9 waiver of attorney-client privilege or work product protection with
10 respect to the assessment and any information contained in the
11 assessment.

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

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

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

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

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

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

3 2. Publicly commit to process such data only in a de-identified
4 fashion and not attempt to reidentify the data; and

5 3. Contractually obligate any recipient of the de-identified
6 data to comply with the requirements of this subsection.

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

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

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

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

16 a. is not reasonably capable of associating the request
17 with the personal data or it would be unreasonably
18 burdensome for the controller to associate the request
19 with the personal data,

20 b. does not use the personal data to recognize or respond
21 to the specific consumer who is the subject of the
22 personal data or associate the personal data with
23 other personal data about the same specific consumer,
24 and

1 c. does not sell the personal data to any third party or
2 otherwise voluntarily disclose the personal data to
3 any third party other than a processor, except as
4 otherwise permitted by this section.

5 C. The consumer rights under paragraphs 1 through 4 of
6 subsection B of Section 2 of this act and controller duties under
7 Section 7 of this act shall not apply to pseudonymous data in cases
8 in which the controller is able to demonstrate any information
9 necessary to identify the consumer is kept separately and is subject
10 to effective technical and organizational controls that prevent the
11 controller from accessing the information.

12 D. A controller that discloses pseudonymous data or de-
13 identified data shall exercise reasonable oversight to monitor
14 compliance with any contractual commitments to which the
15 pseudonymous data or de-identified data is subject and shall take
16 appropriate steps to address any breach of the contractual
17 commitments.

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

21 A. The Attorney General has exclusive authority to enforce the
22 provisions of this act.

23 B. The Attorney General shall post on the Attorney General's
24 Internet website:

1 1. Information relating to:

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

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

4 and

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

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

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

11 Before bringing an action under Section 14 of this act, the
12 Attorney General shall notify the controller or processor in
13 writing, no later than thirty (30) days before bringing the action,
14 identifying the specific provisions of this act that the Attorney
15 General alleges have been or are being violated. The Attorney
16 General shall not bring an action against the controller or
17 processor if:

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

20 2. The controller or processor provides the Attorney General a
21 written statement that the controller or processor:

22 a. cured the alleged violation,

23 b. provided supportive documentation to show how the

24 privacy violation was cured, and

1 c. that no further violations will occur.

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

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

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

- 12 1. Recover a civil penalty under this section;
- 13 2. Restrain or enjoin the person from violating this act; or
- 14 3. Recover the civil penalty and seek injunctive relief.

15 C. The court may award reasonable attorney fees and other
16 expenses incurred in investigating and bringing an action under this
17 section.

18 D. Civil penalties collected in an action under this section
19 shall be deposited in the State Treasury to the credit of the
20 General Revenue Fund.

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

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

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

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

8 2. During a calendar year, either:

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

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

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

16 1. A state agency or a political subdivision of this state, or
17 a service provider processing data on behalf of a state agency or
18 political subdivision of this state;

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

21 3. A covered entity or business associate governed by the
22 privacy, security, and breach notification rules issued by the
23 United States Department of Health and Human Services, 45 C.F.R.,
24 Parts 160 and 164, established under the Health Insurance

1 Portability and Accountability Act of 1996, 42 U.S.C., Section 1320d
2 et seq., and the Health Information Technology for Economic and
3 Clinical Health Act, Division A of Title XIII and Division B of
4 Title IV of the American Recovery and Reinvestment Act of 2009, Pub.
5 L. No. 111-5;

6 4. A nonprofit organization;

7 5. An institution of higher education;

8 6. The processing of personal data by a person in the course of
9 a purely personal or household activity; or

10 7. Personal data collected and used for purposes of the federal
11 policy under the Controlled Substances Act, Section on the
12 Regulation of Listed Chemicals under 21 U.S.C., Section 830, is
13 exempt.

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

17 The following information shall be exempt from this act:

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

21 2. Health records;

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

24 4. Identifiable private information:

- 1 a. for purposes of the federal policy for the protection
2 of human subjects under 45 C.F.R., Part 46,
3 b. collected as part of human subjects research under the
4 good clinical practice guidelines issued by the
5 International Council for Harmonisation of Technical
6 Requirements for Pharmaceuticals for Human Use (ICH)
7 or of the protection of human subjects under 21
8 C.F.R., Parts 50 and 56, or
9 c. that is personal data used or shared in research
10 conducted in accordance with the requirements set
11 forth in this act or other research conducted in
12 accordance with applicable law;

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

16 6. Patient safety work product for purposes of the Patient
17 Safety and Quality Improvement Act of 2005, 42 U.S.C., Section 299b-
18 21 et seq.;

19 7. Information derived from any of the health care-related
20 information listed in this section that is de-identified in
21 accordance with the requirements for de-identification under the
22 Health Insurance Portability and Accountability Act of 1996, 42
23 U.S.C., Section 1320d et seq. or any regulation adopted thereunder;
24

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

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

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

17 11. The collection, maintenance, disclosure, sale,
18 communication, or use of any personal information bearing on a
19 consumer's creditworthiness, credit standing, credit capacity,
20 character, general reputation, personal characteristics, or mode of
21 living by a consumer reporting agency or furnisher that provides
22 information for use in a consumer report, and by a user of a
23 consumer report, but only to the extent that the activity is
24

1 regulated by and authorized under the Fair Credit Reporting Act, 15
2 U.S.C., Section 1681 et seq.;

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

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

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

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

15 16. Data processed or maintained as the emergency contact
16 information of an individual under this act that is used for
17 emergency contact purposes; or

18 17. Data that is processed or maintained and is necessary to
19 retain to administer benefits for another individual that relates to
20 an individual described by paragraph 15 of this section and used for
21 the purposes of administering those benefits.

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

1 A controller or processor that complies with the verifiable
2 parental consent requirements of the Children's Online Privacy
3 Protection Act of 1998 with respect to data collected online shall
4 be considered to be in compliance with any requirement to obtain
5 parental consent under this act.

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

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

11 1. Comply with federal, state, or local laws, rules, or
12 regulations;

13 2. Comply with a civil, criminal, or regulatory inquiry,
14 investigation, subpoena, or summons by federal, state, local, or
15 other governmental authorities;

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

20 4. Investigate, establish, exercise, prepare for, or defend
21 legal claims;

22 5. Provide a product or service specifically requested by a
23 consumer or the parent or guardian of a child, perform a contract to
24 which the consumer is a party, including fulfilling the terms of a

1 written warranty, or take steps at the request of the consumer
2 before entering into a contract;

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

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

10 8. Preserve the integrity or security of systems or
11 investigate, report, or prosecute those responsible for breaches of
12 system security;

13 9. Engage in public or peer-reviewed scientific or statistical
14 research in the public interest that adheres to all other applicable
15 ethics and privacy laws and is approved, monitored, and governed by
16 an institutional review board or similar independent oversight
17 entity that determines:

18 a. if the deletion of the information is likely to
19 provide substantial benefits that do not exclusively
20 accrue to the controller,

21 b. whether the expected benefits of the research outweigh
22 the privacy risks, and

23 c. if the controller has implemented reasonable
24 safeguards to mitigate privacy risks associated with

1 research, including any risks associated with
2 reidentification; or

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

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

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

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

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

15 SECTION 19. NEW LAW A new section of law to be codified
16 in the Oklahoma Statutes as Section 318 of Title 75A, unless there
17 is created a duplication in numbering, reads as follows:

18 A. The requirements imposed on controllers and processors under
19 this act shall not restrict a controller's or processor's ability to
20 collect, use, or retain data to:

21 1. Conduct internal research to develop, improve, or repair
22 products, services, or technology;

23 2. Effect a product recall;

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

3 4. Perform internal operations that are:

4 a. reasonably aligned with the expectations of the
5 consumer,

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

8 c. otherwise compatible with processing data in
9 furtherance of the provision of a product or service
10 specifically requested by a consumer or the
11 performance of a contract to which the consumer is a
12 party.

13 B. A requirement imposed on a controller or processor under
14 this act shall not apply if compliance with the requirement by the
15 controller or processor, as applicable, would violate an evidentiary
16 privilege under the laws of this state.

17 C. The processing of personal data by an entity for the
18 purposes described in subsection A of this section shall not solely
19 make the entity a controller with respect to the processing of the
20 data.

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

1 A. A controller or processor that discloses personal data to a
2 third-party controller or processor, in compliance with the
3 requirements of this act, shall not be deemed to be in violation of
4 this act if the third-party controller or processor that receives
5 and processes that personal data is in violation of this act;
6 provided, that at the time of the data's disclosure, the disclosing
7 controller or processor did not have actual knowledge that the
8 recipient intended to commit a violation.

9 B. A third-party controller or processor receiving personal
10 data from a controller or processor in compliance with the
11 requirements of this act shall not be deemed to be in violation of
12 this act for any wrongdoing of the controller or processor from
13 which the third-party controller or processor receives the personal
14 data.

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

18 A. Personal data processed by a controller pursuant to Section
19 18, 19, or 20 of this act shall not be processed for any purpose
20 other than a purpose listed in Section 18, 19, or 20 of this act
21 unless otherwise allowed by this act. Personal data processed by a
22 controller under Section 18, 19, or 20 of this act may be processed
23 to the extent that the processing of the data is:

24

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

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

6 B. Personal data collected, used, or retained under subsection
7 A of Section 19 of this act shall, where applicable, consider the
8 nature and purpose of such collection, use, or retention. The
9 personal data described by this subsection is subject to reasonable
10 administrative, technical, and physical measures to protect the
11 confidentiality, integrity, and accessibility of the personal data
12 and to reduce reasonably foreseeable risks of harm to consumers
13 relating to the collection, use, or retention of personal data.

14 C. A controller that processes personal data under an exemption
15 in Section 18, 19, or 20 of this act bears the burden of
16 demonstrating that the processing of the personal data qualifies for
17 the exemption and complies with the requirements of subsections A
18 and B of this section.

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

22 SECTION 22. This act shall become effective January 1, 2027."
23
24

1 Passed the House of Representatives the 19th day of February,
2026.

3
4 _____
5 Presiding Officer of the House of
6 Representatives

7 Passed the Senate the ____ day of _____, 2026.

8
9 _____
10 Presiding Officer of the Senate

1 ENGROSSED SENATE
BILL NO. 546

By: Howard of the Senate

2
3 and

4 West (Josh) of the House

5
6 [data privacy - consumer rights - consumer requests
7 - appeal process - exceptions - privacy notice -
disclosures - contracts - data protection assessments
8 - action - penalties - fees and expenses -
evidentiary privileges - liability - codification -
effective date]
9

10

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

12 SECTION 23. NEW LAW A new section of law to be codified
13 in the Oklahoma Statutes as Section 300 of Title 75A, unless there
14 is created a duplication in numbering, reads as follows:

15 As used in this act:

16 1. "Affiliate" means a legal entity that controls, is
17 controlled by, or is under common control with another legal entity
18 or shares common branding with another legal entity. For purposes
19 of this paragraph, "control" or "controlled" means the:

20 a. ownership of, or power to vote, more than fifty
21 percent (50%) of the outstanding shares of any class
22 of voting securities of a company,
23
24

1 b. control in any manner over the election of a majority
2 of the directors or of individuals exercising similar
3 functions, or

4 c. power to exercise controlling influence over the
5 management of a company;

6 2. "Authenticate" means to verify through reasonable means that
7 the consumer who is entitled to exercise the consumer's rights under
8 this act is the same consumer exercising such consumer rights with
9 respect to the personal data at issue;

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

22 4. "Business associate" has the meaning assigned to the term
23 under the Health Insurance Portability and Accountability Act of
24

1 1996, 42 U.S.C., Section 1320d et seq. or any regulation adopted
2 thereunder;

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

5 6. "Children's Online Privacy Protection Act of 1998" means 15
6 U.S.C., Section 6501 et seq. and includes the regulations, rules,
7 guidance, and exemptions adopted pursuant to the act and any
8 subsequent amendments;

9 7. "Consent", when referring to a consumer, means a clear
10 affirmative act signifying a consumer's freely given, specific,
11 informed, and unambiguous agreement to process personal data
12 relating to the consumer. The term includes, but is not limited to,
13 a written statement, including a statement written by electronic
14 means, or any other unambiguous affirmative action. The term does
15 not include:

16 a. acceptance of a general or broad terms of use or
17 similar document that contains descriptions of
18 personal data processing along with other, unrelated
19 information,

20 b. hovering over, muting, pausing, or closing a given
21 piece of content, or

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

23 8. "Consumer" means an individual who is a resident of this
24 state acting only in an individual or household context. The term

1 does not include an individual acting in a commercial or employment
2 context;

3 9. "Controller" means an individual or other person that, alone
4 or jointly with others, determines the purpose and means of
5 processing personal data;

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

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

13 12. "Decision that produces a legal or similarly significant
14 effect concerning a consumer" means a decision made by the
15 controller that results in the provision or denial by the controller
16 of:

- 17 a. financial and lending services,
- 18 b. housing, insurance, or health care services,
- 19 c. education enrollment,
- 20 d. employment opportunities,
- 21 e. criminal justice, or
- 22 f. access to basic necessities such as food and water;

23

24

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

4 14. "Health care provider" has the meaning assigned to the term
5 under the Health Insurance Portability and Accountability Act of
6 1996, 42 U.S.C., Section 1320d et seq.;

7 15. "Health record" means any written, printed, or
8 electronically recorded material maintained by a health care
9 provider in the course of providing health care services to an
10 individual that concerns the individual and the services provided.

11 The term includes:

- 12 a. the substance of any communication made by an
13 individual to a health care provider in confidence
14 during or in connection with the provision of health
15 care services, or
- 16 b. information otherwise acquired by the health care
17 provider about an individual in confidence and in
18 connection with health care services provided to the
19 individual;

20 16. "Identified or identifiable individual" means a consumer
21 who can be readily identified, directly or indirectly;

22 17. "Institution of higher education" means:
23
24

- 1 a. a public institution that is a member of The Oklahoma
- 2 State System of Higher Education or a technology
- 3 center school district, or
- 4 b. a private institution of higher education;

5 18. "Nonprofit organization" means:

- 6 a. a corporation organized under Title 18 of the Oklahoma
- 7 Statutes to the extent applicable to nonprofit
- 8 corporations,
- 9 b. an organization exempt from federal taxation under
- 10 Section 501(a), Internal Revenue Code of 1986, as
- 11 amended, by being listed as an exempt organization
- 12 under Section 501(c) (3), 501(c) (6), or 501(c) (12) of
- 13 that code,
- 14 c. a political organization,
- 15 d. an organization that is:
 - 16 (1) exempt from federal taxation under Section
 - 17 501(a), Internal Revenue Code of 1986, as
 - 18 amended, by being listed as an exempt
 - 19 organization under Section 501(c) (4) of that
 - 20 code, and
 - 21 (2) described by Section 363 of Title 36 of the
 - 22 Oklahoma Statutes, or

1 e. a subsidiary or affiliate of an entity regulated under
2 Section 151 et seq. of Title 17 of the Oklahoma
3 Statutes;

4 19. "Personal data" means any information including sensitive
5 data that is linked or reasonably linkable to an identified or
6 identifiable individual. The term includes pseudonymous data when
7 the data is used by a controller or processor in conjunction with
8 additional information that reasonably links the data to an
9 identified or identifiable individual. The term does not include
10 de-identified data or publicly available information;

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

- 15 a. the selection, nomination, election, or appointment of
16 an individual to a federal, state, or local public
17 office or an office in a political organization,
18 regardless of whether the individual is selected,
19 nominated, elected, or appointed, or
20 b. the election of a presidential/vice-presidential
21 elector, regardless of whether the elector is
22 selected, nominated, elected, or appointed;

23 21. "Precise geolocation data" means information derived from
24 technology, including global positioning system level latitude and

1 longitude coordinates or other mechanisms, that directly identifies
2 the specific location of an individual with precision and accuracy
3 within a radius of one thousand seven hundred fifty (1,750) feet.
4 The term does not include the content of communications nor does it
5 include any data generated by or connected to an advanced utility
6 metering infrastructure system or to equipment for use by a utility;

7 22. "Process" or "processing" means any operation or set of
8 operations performed, whether by manual or automated means, on
9 personal data or on sets of personal data, such as the collection,
10 use, storage, disclosure, analysis, deletion, or modification of
11 personal data;

12 23. "Processor" means a person who, or legal entity that,
13 processes personal data on behalf of a controller;

14 24. "Profiling" means any form of solely automated processing
15 performed on personal data to evaluate, analyze, or predict personal
16 aspects related to an identified or identifiable individual's
17 economic situation, health, personal preferences, interests,
18 reliability, behavior, location, or movements;

19 25. "Protected health information" has the meaning assigned to
20 the term under the Health Insurance Portability and Accountability
21 Act of 1996, 42 U.S.C., Section 1320d et seq. or any regulation
22 adopted thereunder;

23 26. "Pseudonymous data" means personal data that cannot be
24 attributed to a specific individual without the use of additional

1 information, provided that the additional information is kept
2 separately and is subject to appropriate technical and
3 organizational measures to ensure that the personal data is not
4 attributed to an identified or identifiable individual;

5 27. "Publicly available information" means information that is
6 lawfully made available through government records, or information
7 that a business has a reasonable basis to believe is lawfully made
8 available to the general public through widely distributed media, by
9 a consumer, or by a person to whom a consumer has disclosed the
10 information, unless the consumer has restricted the information to a
11 specific audience;

12 28. "Sale of personal data" means the exchange of personal data
13 for monetary consideration by the controller to a third party. The
14 term does not include the:

- 15 a. disclosure of personal data to a processor that
16 processes the personal data on the controller's
17 behalf,
- 18 b. disclosure of personal data to a third party for
19 purposes of providing a product or service requested
20 by the consumer,
- 21 c. disclosure or transfer of personal data to an
22 affiliate of the controller,
- 23 d. disclosure of information or personal data that the
24 consumer:

- 1 (1) (a) intentionally made available to the general
2 public through a mass media channel, and
3 (b) did not restrict to a specific audience, or
4 (2) directs the controller to disclose or
5 intentionally uses the controller to interact
6 with a third party, or
7 e. disclosure or transfer of personal data to a third
8 party as an asset that is part of a proposed or actual
9 merger, acquisition, bankruptcy, or other transaction
10 in which the third party assumes control of all or
11 part of the controller's assets;

12 29. "Sensitive data" means a category of personal data. The
13 term includes:

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

22 30. "State agency" means a department, commission, board,
23 office, council, authority, or other agency in the executive branch
24 of state government that is created by the constitution or a statute

1 of this state, including a public university system or public
2 institution of higher education;

3 31. "Targeted advertising" means displaying to a consumer an
4 advertisement that is selected based on personal data obtained from
5 that consumer's activities over time and across nonaffiliated
6 websites or online applications to predict the consumer's
7 preferences or interests. The term does not include:

8 a. an advertisement that is:

9 (1) based on activities within a controller's own
10 websites or online applications,

11 (2) based on the context of a consumer's current
12 search query, visit to a website, or online
13 application, or

14 (3) directed to a consumer in response to the
15 consumer's request for information or feedback,
16 or

17 b. the processing of personal data solely for measuring
18 or reporting advertising performance, reach, or
19 frequency;

20 32. "Third party" means a person other than the consumer, the
21 controller, the processor, or an affiliate of the controller or
22 processor; and
23
24

1 33. "Trade secret" means information including a formula,
2 pattern, compilation, program, device, method, technique, or
3 process, that:

4 a. derives independent economic value, actual or
5 potential, from not being generally known to, and not
6 being readily ascertainable by proper means by, other
7 persons who can obtain economic value from its
8 disclosure or use, and

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

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

14 A. A consumer is entitled to exercise the consumer rights
15 authorized by this section at any time by submitting a request to a
16 controller specifying the consumer rights the consumer wishes to
17 exercise. With respect to the processing of personal data belonging
18 to a known child, a parent or legal guardian of the child may
19 exercise the consumer rights on behalf of the child.

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

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

1 2. Correct inaccuracies in the consumer's personal data,
2 considering the nature of the personal data and the purposes of the
3 processing of the consumer's personal data;

4 3. Delete personal data provided by or obtained about the
5 consumer;

6 4. If the data is available in a digital format, obtain a copy
7 of the consumer's personal data that the consumer previously
8 provided to the controller in a portable and, to the extent
9 technically feasible, readily usable format that allows the consumer
10 to transmit the data to another controller without hindrance, where
11 the processing is carried out by automated means; or

12 5. Opt out of the processing of the personal data for purposes
13 of:

14 a. targeted advertising,

15 b. the sale of personal data, or

16 c. profiling in furtherance of a decision that produces a
17 legal or similarly significant effect concerning the
18 consumer.

19 SECTION 25. NEW LAW A new section of law to be codified
20 in the Oklahoma Statutes as Section 302 of Title 75A, unless there
21 is created a duplication in numbering, reads as follows:

22 A. Except as otherwise provided by this act, a controller shall
23 comply with a request submitted by a consumer to exercise the
24

1 consumer's rights pursuant to Section 2 of this act as provided by
2 this section.

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

10 C. If a controller declines to take action regarding the
11 consumer's request, the controller shall inform the consumer no
12 later than the forty-five (45) days after the date of receipt of the
13 request of the justification for declining to take action and
14 provide instructions on how to appeal the decision in accordance
15 with Section 4 of this act.

16 D. A controller shall provide information in response to a
17 consumer request free of charge, up to twice annually per consumer.
18 If a request from a consumer is manifestly unfounded, excessive, or
19 repetitive, the controller may charge the consumer a reasonable fee
20 to cover the administrative costs of complying with the request or
21 may decline to act on the request. The controller shall bear the
22 burden of demonstrating for purposes of this subsection that a
23 request is manifestly unfounded, excessive, or repetitive.

24

1 E. If a controller is unable to authenticate the request using
2 commercially reasonable efforts, the controller shall not be
3 required to comply with a consumer request submitted under Section 2
4 of this act and may request that the consumer provide additional
5 information reasonably necessary to authenticate the consumer and
6 the consumer's request.

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

12 1. Retaining a record of the deletion request and the minimum
13 data necessary for the purpose of ensuring the consumer's personal
14 data remains deleted from the business's records and not using the
15 retained data for any other purpose under this act; or

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

19 SECTION 26. NEW LAW A new section of law to be codified
20 in the Oklahoma Statutes as Section 303 of Title 75A, unless there
21 is created a duplication in numbering, reads as follows:

22 A. A controller shall establish a process for a consumer to
23 appeal the controller's refusal to take action on a request within a
24 reasonable period of time after the consumer's receipt of the

1 decision under subsection C of Section 3 of this act. The appeal
2 process shall be conspicuously available and similar to the process
3 for initiating action to exercise consumer rights by submitting a
4 request under Section 2 of this act.

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

13 SECTION 27. NEW LAW A new section of law to be codified
14 in the Oklahoma Statutes as Section 304 of Title 75A, unless there
15 is created a duplication in numbering, reads as follows:

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

20 SECTION 28. NEW LAW A new section of law to be codified
21 in the Oklahoma Statutes as Section 305 of Title 75A, unless there
22 is created a duplication in numbering, reads as follows:

23

24

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

4 1. The ways in which consumers normally interact with the
5 controller;

6 2. The necessity for secure and reliable communications of
7 those requests; and

8 3. The ability of the controller to authenticate the identity
9 of the consumer making the request.

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

13 C. Except as provided by subsection D of this section, if the
14 controller maintains an Internet website, the controller shall
15 provide a mechanism on the website for consumers to submit requests
16 for information required to be disclosed under this act.

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

22 SECTION 29. NEW LAW A new section of law to be codified
23 in the Oklahoma Statutes as Section 306 of Title 75A, unless there
24 is created a duplication in numbering, reads as follows:

1 A. A controller shall:

2 1. Limit the collection of personal data to what is adequate,
3 relevant, and reasonably necessary in relation to the purposes for
4 which that personal data is processed, as disclosed to the consumer;
5 and

6 2. For purposes of protecting the confidentiality, integrity,
7 and accessibility of personal data, establish, implement, and
8 maintain reasonable administrative, technical, and physical data
9 security practices that are appropriate to the volume and nature of
10 the personal data at issue.

11 B. A controller shall not:

12 1. Except as otherwise provided by this act, process personal
13 data for a purpose that is neither reasonably necessary to nor
14 compatible with the disclosed purpose for which the personal data is
15 processed, as disclosed to the consumer, unless the controller
16 obtains the consumer's consent;

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

19 3. Discriminate against a consumer for exercising any consumer
20 rights contained in this act, including by denying goods or
21 services, charging different prices or rates for goods or services,
22 or providing a different level of quality of goods or services to
23 the consumer; or

1 4. Process the sensitive data of a consumer without obtaining
2 the consumer's consent or, in the case of processing the sensitive
3 data of a known child, without processing that data in accordance
4 with the Children's Online Privacy Protection Act of 1998.

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

15 SECTION 30. NEW LAW A new section of law to be codified
16 in the Oklahoma Statutes as Section 307 of Title 75A, unless there
17 is created a duplication in numbering, reads as follows:

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

20 1. The categories of personal data processed by the controller,
21 including, if applicable, any sensitive data processed by the
22 controller;

23 2. The purpose for processing personal data;

24

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

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

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

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

14 SECTION 31. NEW LAW A new section of law to be codified
15 in the Oklahoma Statutes as Section 308 of Title 75A, unless there
16 is created a duplication in numbering, reads as follows:

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

20 1. Taking into account the nature of processing and the
21 information available to the processor, assisting the controller in
22 responding to consumer rights requests submitted under Section 2 of
23 this act by using appropriate technical and organizational measures,
24 as reasonably practicable;

1 2. Taking into account the nature of processing and the
2 information available to the processor, assisting the controller
3 with regard to complying with the requirement relating to the
4 security of processing personal data and to the notification of a
5 breach of security of the processor's system under the Security
6 Breach Notification Act, Section 161 et seq. of Title 24 of the
7 Oklahoma Statutes; and

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

11 B. A contract between a controller and a processor shall govern
12 the processor's data processing procedures with respect to
13 processing performed on behalf of the controller. The contract
14 shall include:

15 1. Clear instructions for processing data;

16 2. The nature and purpose of processing;

17 3. The type of data subject to processing;

18 4. The duration of processing;

19 5. The rights and obligations of both parties; and

20 6. A requirement that the processor shall:

21 a. ensure that each person processing personal data is
22 subject to a duty of confidentiality with respect to
23 the data,

24

- 1 b. at the controller's direction, delete or return all
2 personal data to the controller as requested after the
3 provision of the service is completed, unless
4 retention of the personal data is required by law,
5 c. make available to the controller, upon reasonable
6 request, all information in the processor's possession
7 necessary to demonstrate the processor's compliance
8 with the requirements of this act,
9 d. allow, and cooperate with, reasonable assessments by
10 the controller or the controller's designated
11 assessor, and
12 e. engage any subcontractor pursuant to a written
13 contract that requires the subcontractor to meet the
14 requirements of the processor with respect to the
15 personal data.

16 C. Notwithstanding the requirement described by subparagraph d
17 of paragraph 6 of subsection B of this section, a processor, in the
18 alternative, may arrange for a qualified and independent assessor to
19 conduct an assessment of the processor's policies and technical and
20 organizational measures in support of the requirements under this
21 act using an appropriate and accepted control standard or framework
22 and assessment procedure. The processor shall provide a report of
23 the assessment to the controller on request.

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

5 E. A determination of whether a person is acting as a
6 controller or processor with respect to a specific processing of
7 data is a fact-based determination that depends on the context in
8 which personal data is to be processed. A processor that continues
9 to adhere to a controller's instructions with respect to a specific
10 processing of personal data remains in the role of a processor.

11 SECTION 32. NEW LAW A new section of law to be codified
12 in the Oklahoma Statutes as Section 309 of Title 75A, unless there
13 is created a duplication in numbering, reads as follows:

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

17 1. The processing of personal data for purposes of targeted
18 advertising;

19 2. The sale of personal data;

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

22 a. unfair or deceptive treatment of or unlawful disparate
23 impact on consumers,

24

- b. financial, physical, or reputational injury to consumers,
- c. a physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person, or
- d. other substantial injury to consumers;

4. The processing of sensitive data; and

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

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

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

2. Factor into the assessment the:

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

1 C. A controller shall make a data protection assessment
2 available to the Attorney General upon written request pursuant to a
3 civil investigation demand.

4 D. A data protection assessment shall be confidential and
5 exempt from public inspection and copying under the Oklahoma Open
6 Records Act, Section 24A.1 et seq. of Title 51 of the Oklahoma
7 Statutes. Disclosure of a data protection assessment in compliance
8 with a request from the Attorney General shall not constitute a
9 waiver of attorney-client privilege or work product protection with
10 respect to the assessment and any information contained in the
11 assessment.

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

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

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

21 SECTION 33. NEW LAW A new section of law to be codified
22 in the Oklahoma Statutes as Section 310 of Title 75A, unless there
23 is created a duplication in numbering, reads as follows:

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

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

3 2. Publicly commit to process such data only in a de-identified
4 fashion and not attempt to reidentify the data; and

5 3. Contractually obligate any recipient of the de-identified
6 data to comply with the requirements of this subsection.

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

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

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

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

16 a. is not reasonably capable of associating the request
17 with the personal data or it would be unreasonably
18 burdensome for the controller to associate the request
19 with the personal data,

20 b. does not use the personal data to recognize or respond
21 to the specific consumer who is the subject of the
22 personal data or associate the personal data with
23 other personal data about the same specific consumer,
24 and

1 c. does not sell the personal data to any third party or
2 otherwise voluntarily disclose the personal data to
3 any third party other than a processor, except as
4 otherwise permitted by this section.

5 C. The consumer rights under paragraphs 1 through 4 of
6 subsection B of Section 2 of this act and controller duties under
7 Section 7 of this act shall not apply to pseudonymous data in cases
8 in which the controller is able to demonstrate any information
9 necessary to identify the consumer is kept separately and is subject
10 to effective technical and organizational controls that prevent the
11 controller from accessing the information.

12 D. A controller that discloses pseudonymous data or de-
13 identified data shall exercise reasonable oversight to monitor
14 compliance with any contractual commitments to which the
15 pseudonymous data or de-identified data is subject and shall take
16 appropriate steps to address any breach of the contractual
17 commitments.

18 SECTION 34. NEW LAW A new section of law to be codified
19 in the Oklahoma Statutes as Section 311 of Title 75A, unless there
20 is created a duplication in numbering, reads as follows:

21 A. The Attorney General has exclusive authority to enforce the
22 provisions of this act.

23 B. The Attorney General shall post on the Attorney General's
24 Internet website:

1 1. Information relating to:

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

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

4 and

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

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

8 SECTION 35. NEW LAW A new section of law to be codified
9 in the Oklahoma Statutes as Section 312 of Title 75A, unless there
10 is created a duplication in numbering, reads as follows

11 Before bringing an action under Section 14 of this act, the
12 Attorney General shall notify the controller or processor in
13 writing, no later than thirty (30) days before bringing the action,
14 identifying the specific provisions of this act that the Attorney
15 General alleges have been or are being violated. The Attorney
16 General shall not bring an action against the controller or
17 processor if:

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

20 2. The controller or processor provides the Attorney General a
21 written statement that the controller or processor:

22 a. cured the alleged violation,

23 b. provided supportive documentation to show how the

24 privacy violation was cured, and

1 c. that no further violations will occur.

2 SECTION 36. NEW LAW A new section of law to be codified
3 in the Oklahoma Statutes as Section 313 of Title 75A, unless there
4 is created a duplication in numbering, reads as follows:

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

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

- 12 1. Recover a civil penalty under this section;
- 13 2. Restrain or enjoin the person from violating this act; or
- 14 3. Recover the civil penalty and seek injunctive relief.

15 C. The court may award reasonable attorney fees and other
16 expenses incurred in investigating and bringing an action under this
17 section.

18 D. Civil penalties collected in an action under this section
19 shall be deposited in the State Treasury to the credit of the
20 General Revenue Fund.

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

1 SECTION 37. NEW LAW A new section of law to be codified
2 in the Oklahoma Statutes as Section 314 of Title 75A, unless there
3 is created a duplication in numbering, reads as follows:

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

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

8 2. During a calendar year, either:

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

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

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

16 1. A state agency or a political subdivision of this state, or
17 a service provider processing data on behalf of a state agency or
18 political subdivision of this state;

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

21 3. A covered entity or business associate governed by the
22 privacy, security, and breach notification rules issued by the
23 United States Department of Health and Human Services, 45 C.F.R.,
24 Parts 160 and 164, established under the Health Insurance

1 Portability and Accountability Act of 1996, 42 U.S.C., Section 1320d
2 et seq., and the Health Information Technology for Economic and
3 Clinical Health Act, Division A of Title XIII and Division B of
4 Title IV of the American Recovery and Reinvestment Act of 2009, Pub.
5 L. No. 111-5;

6 4. A nonprofit organization;

7 5. An institution of higher education; or

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

10 SECTION 38. NEW LAW A new section of law to be codified
11 in the Oklahoma Statutes as Section 315 of Title 75A, unless there
12 is created a duplication in numbering, reads as follows:

13 The following information shall be exempt from this act:

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

17 2. Health records;

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

20 4. Identifiable private information:

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

23 b. collected as part of human subjects research under the
24 good clinical practice guidelines issued by the

1 International Council for Harmonisation of Technical
2 Requirements for Pharmaceuticals for Human Use (ICH)
3 or of the protection of human subjects under 21
4 C.F.R., Parts 50 and 56, or

5 c. that is personal data used or shared in research
6 conducted in accordance with the requirements set
7 forth in this act or other research conducted in
8 accordance with applicable law;

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

12 6. Patient safety work product for purposes of the Patient
13 Safety and Quality Improvement Act of 2005, 42 U.S.C., Section 299b-
14 21 et seq.;

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

20 8. Information originating from, and intermingled to be
21 indistinguishable with, or information treated in the same manner
22 as, information exempt under this section that is maintained by a
23 covered entity or business associate as defined under the Health
24 Insurance Portability and Accountability Act of 1996, 42 U.S.C.,

1 Section 1320d et seq. or any regulation adopted thereunder, or by a
2 program or a qualified service organization as defined under 42
3 U.S.C., Section 290dd-2 or any regulation adopted thereunder;

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

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

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

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

24

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

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

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

10 16. Data processed or maintained as the emergency contact
11 information of an individual under this act that is used for
12 emergency contact purposes; or

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

17 SECTION 39. NEW LAW A new section of law to be codified
18 in the Oklahoma Statutes as Section 316 of Title 75A, unless there
19 is created a duplication in numbering, reads as follows:

20 A controller or processor that complies with the verifiable
21 parental consent requirements of the Children's Online Privacy
22 Protection Act of 1998 with respect to data collected online shall
23 be considered to be in compliance with any requirement to obtain
24 parental consent under this act.

1 SECTION 40. NEW LAW A new section of law to be codified
2 in the Oklahoma Statutes as Section 317 of Title 75A, unless there
3 is created a duplication in numbering, reads as follows:

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

6 1. Comply with federal, state, or local laws, rules, or
7 regulations;

8 2. Comply with a civil, criminal, or regulatory inquiry,
9 investigation, subpoena, or summons by federal, state, local, or
10 other governmental authorities;

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

15 4. Investigate, establish, exercise, prepare for, or defend
16 legal claims;

17 5. Provide a product or service specifically requested by a
18 consumer or the parent or guardian of a child, perform a contract to
19 which the consumer is a party, including fulfilling the terms of a
20 written warranty, or take steps at the request of the consumer
21 before entering into a contract;

22 6. Take immediate steps to protect an interest that is
23 essential for the life or physical safety of the consumer or of
24

1 another individual and in which the processing cannot be manifestly
2 based on another legal basis;

3 7. Prevent, detect, protect against, or respond to security
4 incidents, identity theft, fraud, harassment, malicious or deceptive
5 activities, or any illegal activity;

6 8. Preserve the integrity or security of systems or
7 investigate, report, or prosecute those responsible for breaches of
8 system security;

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

- 14 a. if the deletion of the information is likely to
15 provide substantial benefits that do not exclusively
16 accrue to the controller,
- 17 b. whether the expected benefits of the research outweigh
18 the privacy risks, and
- 19 c. if the controller has implemented reasonable
20 safeguards to mitigate privacy risks associated with
21 research, including any risks associated with
22 reidentification; or

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

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

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

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

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

11 SECTION 41. NEW LAW A new section of law to be codified
12 in the Oklahoma Statutes as Section 318 of Title 75A, unless there
13 is created a duplication in numbering, reads as follows:

14 A. The requirements imposed on controllers and processors under
15 this act shall not restrict a controller's or processor's ability to
16 collect, use, or retain data to:

17 1. Conduct internal research to develop, improve, or repair
18 products, services, or technology;

19 2. Effect a product recall;

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

22 4. Perform internal operations that are:

23 a. reasonably aligned with the expectations of the
24 consumer,

- 1 b. reasonably anticipated based on the consumer's
2 existing relationship with the controller, or
3 c. otherwise compatible with processing data in
4 furtherance of the provision of a product or service
5 specifically requested by a consumer or the
6 performance of a contract to which the consumer is a
7 party.

8 B. A requirement imposed on a controller or processor under
9 this act shall not apply if compliance with the requirement by the
10 controller or processor, as applicable, would violate an evidentiary
11 privilege under the laws of this state.

12 C. The processing of personal data by an entity for the
13 purposes described in subsection A of this section shall not solely
14 make the entity a controller with respect to the processing of the
15 data.

16 SECTION 42. NEW LAW A new section of law to be codified
17 in the Oklahoma Statutes as Section 319 of Title 75A, unless there
18 is created a duplication in numbering, reads as follows:

19 A. A controller or processor that discloses personal data to a
20 third-party controller or processor, in compliance with the
21 requirements of this act, shall not be deemed to be in violation of
22 this act if the third-party controller or processor that receives
23 and processes that personal data is in violation of this act;
24 provided, that at the time of the data's disclosure, the disclosing

1 controller or processor did not have actual knowledge that the
2 recipient intended to commit a violation.

3 B. A third-party controller or processor receiving personal
4 data from a controller or processor in compliance with the
5 requirements of this act shall not be deemed to be in violation of
6 this act for any wrongdoing of the controller or processor from
7 which the third-party controller or processor receives the personal
8 data.

9 SECTION 43. NEW LAW A new section of law to be codified
10 in the Oklahoma Statutes as Section 320 of Title 75A, unless there
11 is created a duplication in numbering, reads as follows:

12 A. Personal data processed by a controller pursuant to Section
13 18, 19, or 20 of this act shall not be processed for any purpose
14 other than a purpose listed in Section 18, 19, or 20 of this act
15 unless otherwise allowed by this act. Personal data processed by a
16 controller under Section 18, 19, or 20 of this act may be processed
17 to the extent that the processing of the data is:

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

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

23 B. Personal data collected, used, or retained under subsection
24 A of Section 19 of this act shall, where applicable, consider the

1 nature and purpose of such collection, use, or retention. The
2 personal data described by this subsection is subject to reasonable
3 administrative, technical, and physical measures to protect the
4 confidentiality, integrity, and accessibility of the personal data
5 and to reduce reasonably foreseeable risks of harm to consumers
6 relating to the collection, use, or retention of personal data.

7 C. A controller that processes personal data under an exemption
8 in Section 18, 19, or 20 of this act bears the burden of
9 demonstrating that the processing of the personal data qualifies for
10 the exemption and complies with the requirements of subsections A
11 and B of this section.

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

15 SECTION 44. This act shall become effective July 1, 2026.

16
17
18
19
20
21
22
23
24

