ENGROSSED SENATE
BILL NO. 546 By: Howard of the Senate

and

West (Josh) of the House

[data privacy - consumer rights - consumer requests - appeal process - exceptions - privacy notice - disclosures - contracts - data protection assessments - action - penalties - fees and expenses - evidentiary privileges - liability - codification - 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 that is used to identify a specific individual. The term includes, but is not limited to, a fingerprint, voiceprint, eye retina or iris, or other unique biological pattern or characteristic. 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.;

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

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

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

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

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

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

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

c. agreement obtained through the use of dark patterns;

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

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

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

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

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

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

a. financial and lending services,

b. housing, insurance, or health care services,

c. education enrollment,

d. employment opportunities,

e. criminal justice, or

f. access to basic necessities such as food and water;

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

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

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

a. the substance of any communication made by an individual to a health care provider in confidence during or in connection with the provision of health care services, or

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

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

17. "Institution of higher education" means:

a. a public institution that is a member of The Oklahoma State System of Higher Education or a technology center school district, or

b. a private institution of higher education;

18. "Nonprofit organization" means:

a. a corporation organized under Title 18 of the Oklahoma Statutes to the extent applicable to nonprofit corporations,

b. an organization exempt from federal taxation under Section 501(a), Internal Revenue Code of 1986, as amended, by being listed as an exempt organization under Section 501(c)(3), 501(c)(6), or 501(c)(12) of that code,

c. a political organization,

d. an organization that is:

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

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

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

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

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

a. the selection, nomination, election, or appointment of an individual to a federal, state, or local public office or an office in a political organization, regardless of whether the individual is selected, nominated, elected, or appointed, or

b. the election of a presidential/vice-presidential elector, regardless of whether the elector is selected, nominated, elected, or appointed;

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

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

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

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

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

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

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

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

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

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

a. disclosure of personal data to a processor that processes the personal data on the controller's behalf,

b. disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer,

c. disclosure or transfer of personal data to an affiliate of the controller,

d. disclosure of information or personal data that the consumer:

(1) (a) intentionally made available to the general public through a mass media channel, and

(b) did not restrict to a specific audience, or

(2) directs the controller to disclose or intentionally uses the controller to interact with a third party, or

e. disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets;

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

a. personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status,

b. genetic or biometric data that is processed for the purpose of uniquely identifying an individual,

c. personal data collected from a known child, or

d. precise geolocation data;

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

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

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

a. an advertisement that is:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. targeted advertising,

b. the sale of personal data, or

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. A controller shall:

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

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

B. A controller shall not:

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

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

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

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

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

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

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

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

2. The purpose for processing personal data;

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

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

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

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

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

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

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

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

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

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

1. Clear instructions for processing data;

2. The nature and purpose of processing;

3. The type of data subject to processing;

4. The duration of processing;

5. The rights and obligations of both parties; and

6. A requirement that the processor shall:

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

b. at the controller's direction, delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law,

c. make available to the controller, upon reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with the requirements of this act,

d. allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, and

e. engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data.

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

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

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

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

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

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

2. The sale of personal data;

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

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

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

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

d. other substantial injury to consumers;

4. The processing of sensitive data; and

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

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

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

2. Factor into the assessment 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.

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

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

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

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

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

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

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

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

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

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

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

1. Reidentify de-identified data or pseudonymous data;

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

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

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

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

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

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

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

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

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

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

1. Information relating to:

a. the responsibilities of a controller under this act,

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

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

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

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

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

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

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

a. cured the alleged violation,

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

c. that no further violations will occur.

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

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

B. The Attorney General may bring an action to:

1. Recover a civil penalty under this section;

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

3. Recover the civil penalty and seek injunctive relief.

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

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

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

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

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

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

2. During a calendar year, either:

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

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

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

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

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

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

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

4. A nonprofit organization;

5. An institution of higher education; or

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

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

The following information shall be exempt from this act:

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

2. Health records;

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

4. Identifiable private information:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c. if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

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

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

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

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

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

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

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

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

2. Effect a product recall;

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

4. Perform internal operations that are:

a. reasonably aligned with the expectations of the consumer,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SECTION 22. This act shall become effective July 1, 2026.

Passed the Senate the 26th day of March, 2025.

_____
Presiding Officer of the Senate

Passed the House of Representatives the ____ day of _____, 2025.

_____
Presiding Officer of the House of Representatives