HB351

XDP66ZZ-2

By Representative Shaw

RFD: Commerce and Small Business

First Read: 29-Jan-26

A BILL

TO BE ENTITLED

AN ACT

Relating to data privacy; to authorize a consumer to take certain actions regarding the consumer's personal data; to regulate the manner in which a controller may process personal data; to provide for the obligations of a data processor; to regulate the processing of deidentified data; and to provide for enforcement of this act.

BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

Section 1. This act shall be known as the Alabama Personal Data Protection Act.

Section 2. For the purposes of this act, the following terms have the following meanings:

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

(2) AUTHENTICATE. To use reasonable methods to determine that a request to exercise any of the consumer rights afforded under this act is being made by, or on behalf of, a consumer who is entitled to exercise those consumer rights with respect to the consumer's personal data at issue.

(3) BIOMETRIC DATA. Data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, retina, or iris, that are used to identify a specific individual. The term does not include any of the following:

a. A digital or physical photograph.

b. An audio or video recording.

c. Any data generated from paragraph a. or b. unless the data is used to identify a specific individual.

(4) CHILD. An individual under 13 years of age.

(5) CONSENT. A clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer, including, but not limited to, a written statement or a statement by electronic means. The term does not include any of the following:

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

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

c. An agreement obtained using dark patterns.

(6) CONSUMER. An individual who is a resident of this state. The term does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency whose communications or transactions with the controller occur

solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit, or government agency.

(7) CONTROL. Any of the following:

a. Ownership of or the power to vote more than 50 percent of the outstanding shares of any class of voting security of a company.

b. Control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

c. The power to exercise controlling influence over the management of a company.

(8) CONTROLLER. An individual or legal entity that, alone or jointly with others, determines the purposes and means of processing personal data.

(9) DARK PATTERN. A user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice.

(10) DEIDENTIFIED DATA. Data that cannot be used to reasonably infer information about or otherwise be linked to an identified or identifiable individual or a device linked to an identified or identifiable individual if the controller that possesses the data does all of the following:

a. Takes reasonable measures to ensure that the data cannot be associated with an individual.

b. Publicly commits to process the data in a deidentified fashion only and to not attempt to reidentify the data.

c. Contractually obligates any recipients of the data to satisfy the criteria set forth in Section 11(a) and (b).

(11) IDENTIFIABLE INDIVIDUAL. An individual who can be readily identified, directly or indirectly.

(12) NONPROFIT ENTITY. As defined in Section 10A-1-1.03, Code of Alabama 1975.

(13) PERSONAL DATA. Any information that is linked or reasonably linkable to an identified or identifiable individual. The term does not include deidentified data or publicly available information.

(14) PRECISE GEOLOCATION DATA. Information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates, which directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. The term does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(15) PROCESS. Any operation or set of operations, whether by manual or automated means, performed on personal data or on sets of personal data, including, but not limited to, the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(16) PROCESSOR. An individual or legal entity that processes personal data on behalf of a controller.

(17) PROFILING. 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.

(18) PSEUDONYMOUS DATA. Personal data that cannot be attributed to a specific individual without the use of additional information, provided the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributable to an identified or identifiable individual.

(19) PUBLICLY AVAILABLE INFORMATION. Either of the following:

a. Information that is lawfully made available through federal, state, or local government records or widely distributed media.

b. Information that a controller has a reasonable basis to believe a consumer has lawfully made available to the public.

(20) SALE OF PERSONAL DATA. The exchange of personal data for monetary consideration by a controller to a third party, or for other valuable consideration by a controller to a third party where the controller receives a material benefit and the third party is not restricted in its subsequent uses of the personal data. The term does not include any of the following:

a. The disclosure of personal data to a processor that processes the personal data on behalf of the controller.

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

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

d. The disclosure of personal data in which the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party.

e. The disclosure of personal data that the consumer intentionally made available to the public via a channel of mass media and did not restrict to a specific audience.

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

g. The disclosure or transfer of personal data to a third party for the purposes of providing analytics or marketing services solely to the controller.

(21) SENSITIVE DATA. Personal data that includes any of the following:

a. Data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, information about an individual's sex life, sexual orientation, or citizenship or immigration status.

b. The processing of genetic or biometric data for the purpose of uniquely identifying an individual.

c. Personal data collected from a known child.

d. Precise geolocation data.

(22) SIGNIFICANT DECISION. A decision made by a controller that results in the provision or denial by the controller of credit or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunity, health care service, or access to basic necessities such as food or water.

(23) TARGETED ADVERTISING. Displaying advertisements to a consumer in which the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet websites or online applications to predict the consumer's preferences or interests. The term does not include any of the following:

a. Advertisements based on activities within a controller's own Internet websites or online applications.

b. Advertisements based on the context of a consumer's current search query or visit to any Internet website or online application.

c. Advertisements directed to a consumer in response to the consumer's request for information or feedback.

d. Processing personal data solely to measure or report advertising frequency, performance, or reach.

(24) THIRD PARTY. An individual or legal entity other than a consumer, controller, processor, or an affiliate of the controller or processor.

(25) TRADE SECRET. As defined in Section 8-27-2, Code of Alabama 1975.

Section 3. The provisions of this act apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that meet either of the following qualifications:

(1) Control or process the personal data of more than 25,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction.

(2) Derive more than 25 percent of gross revenue from the sale of personal data, regardless of the number of consumers whose data the person controls or processes.

Section 4. (a) Notwithstanding any other provisions of this act, this act shall not apply to any of the following:

(1)a. A political subdivision of the state.

b. A public corporation organized pursuant to Title 11, Code of Alabama 1975.

(2) A two-year or four-year institution of higher education, including affiliates of a two-year or four-year institution of higher education.

(3) A national securities association that is registered under 15 U.S.C. § 78o-3.

(4) A financial institution or an affiliate of a financial institution governed by 15 U.S.C. Chapter 94.

(5) A financial institution or an affiliate of a financial institution governed by, or personal data collected, processed, sold, or disclosed in accordance with Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et. seq.

(6) A covered entity or business associate as defined in the privacy regulations of 45 C.F.R. § 160.103.

(7) A business with fewer than 500 employees, provided the business does not engage in the sale of personal data.

(8) A nonprofit entity, as defined in Section 10A-1-1.03, Code of Alabama 1975, with less than 100 employees, provided the entity does not engage in the sale of personal data.

(9) Any person or entity regulated by Chapter 6 of Title 8, Code of Alabama 1975.

(10) Any person or entity regulated by Chapter 7A of Title 8, Code of Alabama 1975.

(11) Any trade association explicitly authorized to receive documents or evidence pursuant to Section 27-12A-23, Code of Alabama 1975.

(b) This act shall not apply to any of the following information or data:

(1) Protected health information under the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996 and related regulations.

(2) Patient-identifying information for the purposes of 42 C.F.R. Part 2, established pursuant to 42 U.S.C. § 290dd-2.

(3) Identifiable private information for the purposes of 45 C.F.R. Part 46.

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

(5) The protection of human subjects under 21 C.F.R.

Parts 50 and 56, or personal data used or shared in research as defined in the federal Health Insurance Portability and Accountability Act of 1996 and 45 C.F.R. § 164.501, that is conducted in accordance with applicable law.

(6) Information or documents created for the purposes of the federal Health Care Quality Improvement Act of 1986.

(7) Patient safety work products for the purposes of the federal Patient Safety and Quality Improvement Act of 2005.

(8) Information derived from any of the health care related information listed in this subsection which is deidentified in accordance with the requirements for deidentification pursuant to the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996.

(9) Information derived from any of the health care related information listed in this subsection which is included in a limited data set as described in 45 C.F.R. § 164.514(e), to the extent that the information is used, disclosed, and maintained in a manner specified in 45 C.F.R. § 164.514(e).

(10) Information originating from and intermingled to be indistinguishable with or information treated in the same manner as information exempt under this subsection which is maintained by a covered entity or business associate as defined in the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996 or a program or qualified service organization as specified in 42

U.S.C. § 290dd-2.

(11) Information used for public health activities and purposes as authorized by the federal Health Insurance Portability and Accountability Act of 1996, community health activities, and population health activities.

(12) The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user 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 federal Fair Credit Reporting Act.

(13) Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994.

(14) Personal data regulated by the federal Family Educational Rights and Privacy Act of 1974.

(15) Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act of 1971.

(16) Data processed or maintained by an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party to the extent that the data is collected and used within the context of that role.

(17) Data processed or maintained as the emergency

contact information of an individual under this act and used for emergency contact purposes.

(18) Data processed or maintained that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under this section and is used for the purposes of administering the benefits.

(19) Personal data collected, processed, sold, or disclosed in relation to price, route, or service, as these terms are used in the federal Airline Deregulation Act of 1978 by an air carrier subject to the act.

(20) Data or information collected or processed to comply with or in accordance with state law.

(21) Personal data collected or used pursuant to 21 U.S.C. § 830.

(c) Controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act of 1998 are compliant with any obligation to obtain parental consent pursuant to this act.

Section 5. (a) Subject to authentication and any other conditions or limitations provided by this act, a consumer may invoke the rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer right the consumer seeks to invoke. A controller shall comply with an authenticated request to do any of the following:

(1) Confirm whether a controller, or a processor or

third party acting on a controller's behalf, is processing the consumer's personal data and accessing any of the consumer's personal data under the control of the controller, unless confirmation or access would require the controller to reveal a trade secret.

(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) Direct a controller to delete the consumer's personal data.

(4) Obtain a copy of the consumer's personal data previously provided by the consumer to a controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another controller without hindrance when the processing is carried out by automated means, unless the provision of the data would require the controller to reveal a trade secret.

(5) Opt out of the processing of the consumer's personal data for any of the following purposes:

a. Targeted advertising.

b. The sale of the consumer's personal data.

c. Profiling in furtherance of solely automated significant decisions concerning the consumer.

(b) A controller shall establish a secure and reliable method for a consumer to exercise rights established by this section and shall describe the method in the controller's privacy notice.

(c)(1) A parent or legal guardian of a known child may exercise the consumer's rights on behalf of the known child regarding the processing of personal data.

(2) A guardian or conservator of a consumer may exercise the consumer's rights on behalf of the consumer regarding the processing of personal data.

(d) Except as otherwise provided in this act, a controller shall comply with a request by a consumer to exercise the consumer's rights authorized by this section as follows:

(1)a. A controller shall respond to a consumer's request within 45 days of receipt of the request.

b. A controller may extend the response period by 45 additional days, when reasonably necessary considering the complexity and number of the consumer's requests, by notifying the consumer of the extension and the reason for the extension within the initial 45-day response period.

(2) If a controller declines to act regarding a consumer's request, the controller shall inform the consumer of the justification for declining to act within 45 days of receipt of the request.

(3) Information provided in response to a consumer request must be provided by a controller, free of charge, once for each consumer during any 12-month period. If a consumer's requests are manifestly unfounded, excessive, technically infeasible, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with a request or decline to act on a request. Upon

inquiry by an enforcement authority, the controller bears the burden of demonstrating the manifestly unfounded, excessive, technically infeasible, or repetitive nature of a request.

(4) If a controller is unable to authenticate a consumer's request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request until the consumer provides additional information reasonably necessary to authenticate the consumer and the request. A controller is not required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent or otherwise not authorized. If a controller denies an opt-out request because the controller believes the request is fraudulent or not authorized, the controller shall send notice to the person who made the request disclosing that the controller believes the request is fraudulent or not authorized and that the controller may not comply with the request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer is in compliance with a consumer's request to delete the consumer's data if the controller has done either of the following:

a. Retained 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 controller's records and refrains from using the retained data for any other purpose.

b. Opted the consumer out of any further processing of the consumer's personal data for any purpose except for those exempted pursuant to this act.

Section 6. (a) A parent or legal guardian of a known child or a guardian or conservator of a consumer may act on the known child's or the consumer's behalf to opt out of the processing of the known child's or the consumer's personal data for one or more of the purposes specified in Section 5.

(b) A controller must allow a consumer to opt-out through either of the following methods:

(1) By providing a clear and conspicuous link on the controller's Internet website to an Internet web page that enables a consumer directly to opt out of any processing of the consumer's personal data for the purposes of targeted advertising or sale of the consumer's personal data, or provides up-to-date contact information for a consumer to submit the opt-out request.

(2) By January 1, 2028, responding to a consumer's request to opt out of any processing of the consumer's personal data for the purposes of targeted advertising or sale of the consumer's personal data sent through an opt-out preference signal with the consumer's consent, to the controller by a platform, technology, or mechanism that does all of the following:

a. May not unfairly disadvantage another controller.

b. Must require the consumer to affirmatively enable the opt-out preference signal to opt out of any personal data processing pursuant to this act.

c. Must be reasonably consumer friendly and easy to use by the average consumer.

d. Must be consistent with any federal or state law or regulation.

e. Must be designed to allow the controller to accurately determine whether the consumer is a resident of the state and whether the consumer has made a legitimate request to opt out of any sale of a consumer's personal data or targeted advertising.

(c)(1) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of personal data, through an opt-out preference signal sent in accordance with this section conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts, or club card program, the controller shall comply with the consumer's opt-out preference signal but may notify the consumer of the conflict and provide the choice to confirm controller-specific privacy settings or participation in such a program.

(2) If a controller responds to consumer opt-out requests received in accordance with this section by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to this section for the

retention, use, sale, or sharing of the consumer's personal data.

Section 7. (a) A controller shall do all of the following:

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

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

(3) Provide an effective mechanism for a consumer to revoke the consumer's consent under this act that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, on revocation of the consent, cease to further process the personal data as soon as practicable, but no later than 45 days after complying with the consumer's opt-out request consistent with this act.

(b) A controller may not do any of the following:

(1) Except as provided in this act, process personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes for which the personal data is processed as disclosed by the controller.

(2) Process sensitive data concerning a consumer other than a known child without obtaining that consumer's consent or, in the case of the processing of personal data concerning a known child, without processing the data in accordance with

the federal Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 et seq.

(3) Process personal data in violation of the laws of this state or federal laws that prohibit unlawful discrimination against consumers.

(4) Process the personal data of a consumer for the purposes of targeted advertising or sell a consumer's personal data without the consumer's consent under circumstances in which a controller has actual knowledge that the consumer is at least 13 years of age but younger than 16 years of age.

(5) Deny goods or services, charge different prices or rates for goods or services, or provide a different level of quality of goods or services to a consumer if the consumer opts out of the processing of the consumer's data. However, if a consumer opts out of data processing, the covered entity is not required to provide a service that requires data processing. Controllers may provide different prices or levels for goods or services if the good or service is a bona fide loyalty, rewards, premium features, discount, or club card program in which a consumer voluntarily participates.

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

(d) A controller shall provide consumers with a reasonably accurate, clear, and meaningful privacy notice that includes all of the following:

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

(2) The purpose for processing personal data.

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

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

(5) An active email address or other mechanism that the consumer may use to contact the controller.

(6) How consumers may exercise their consumer rights, including a link or contact information for availing themselves of the opt-out method provided in Section 6.

(e)(1) A controller shall establish and describe in a privacy notice one or more secure and reliable means for consumers to submit a request to exercise their consumer rights, as established under Section 5, pursuant to this act considering the ways in which consumers normally interact with the controller, the need for secure and reliable communication of consumer requests, and the ability of the controller to authenticate the identity of the consumer or authorized agent making the request.

(2) A controller may not require a consumer to create a new account to exercise consumer rights but may require a consumer to use an existing account as a means of exercising his or her consumer rights.

(f) Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's consumer rights as established under this act shall be deemed contrary to public policy and shall be void and unenforceable.

Section 8. (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this act, considering the nature of processing and the information available to the processor, including, but not limited to, both of the following:

(1) Maintaining appropriate and reasonably practical technical and organizational measures to support the fulfillment of the controller's obligation to respond to consumer rights requests.

(2) Assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor to meet both the controller's and the processor's obligations.

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

(2) The contract shall:

a. Be binding;

b. Clearly set forth instructions for processing data;

c. Clearly set forth the nature and purpose of the processing;

d. Clearly set forth the type of data subject to processing;

e. Clearly set forth the duration of processing; and

f. Clearly set forth the rights and obligations of both parties.

(3) The contract, taking into account the nature of the processing, the relationship between the parties, and other factors, shall also require the processor to:

a. Ensure that each processor of personal data is subject to a duty of confidentiality with respect to the personal data;

b. Delete or return all personal data to the controller as requested at the end of the provision of services at the controller's direction, unless retention of the personal data is required or permitted by law or the contract;

c. Make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations of this act upon the reasonable request of the controller; and

d. Obligate any subcontractor processing personal data to meet the obligations of the processor with respect to the personal data.

(c) Nothing in this section may be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship as described in this act.

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends on the following context in which personal data is to be processed:

(1) A person who is not limited in the processing of personal data pursuant to a controller's instructions or who fails to adhere to a controller's instructions is a controller and not a processor with respect to a specific processing of data.

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

(3) If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under this act.

Section 9. (a) Any controller in possession of deidentified data shall do all of the following:

(1) Take measures to ensure that the deidentified data cannot reasonably be associated with an individual.

(2) Refrain from reidentifying the deidentified data when maintaining and using deidentified data.

(3) Contractually obligate any recipients of the deidentified data to comply with all provisions of this section.

(b) Nothing in this act may be construed to require a controller to do any of the following:

(1) Reidentify deidentified data or pseudonymous data.

(2) Maintain deidentified data in an identifiable form.

(3) Collect, obtain, retain, or access any identifiable data associated with deidentified data solely for purposes of

authenticating a potential consumer request regarding personal data.

(c) Nothing in this act may be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller or processor:

(1) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome to associate the request with the personal data;

(2) 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

(3) 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 or subprocessor, except as otherwise permitted in this section.

(d) The rights afforded under Section 5 may not apply to pseudonymous data in cases in which the controller is able to demonstrate that 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.

(e) A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Section 10. (a) Nothing in this act may be construed to restrict a controller's or processor's ability to do any of the following:

(1) Comply with federal, state, or local ordinances or regulations.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other government authority.

(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 ordinances, rules, or regulations.

(4) Investigate, establish, exercise, prepare for, or defend legal claims, or otherwise protect the legal rights of the controller or processor.

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

(6) Perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty.

(7) Take steps at the request of a consumer prior to entering a contract.

(8) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and when the processing cannot be manifestly based on another legal basis.

(9) Prevent, detect, protect against, or respond to security incidents; identify theft, including identity theft, fraud, harassment, malicious or deceptive activities, or any

illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any of these actions.

(10) 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 that determines, or similar independent oversight entities that determine, all of the following:

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

b. The expected benefits of the research outweigh the privacy risks.

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

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

(12) Process personal data for reasons of public interest in public health, community health, or population health, but solely to the extent that the processing is both of the following:

a. Subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed.

b. Under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

(b) The obligations imposed on controllers or processors under this act may not restrict a controller's or processor's ability to collect, use, or retain personal data for internal use to do any of the following:

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

(2) Effectuate a product recall.

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

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

(c) The obligations imposed on controllers or processors under this act may not apply when compliance by the controller or processor with this act would violate an evidentiary privilege under the laws of this state. Nothing in this act may be construed 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.

(d)(1) If, at the time a controller or processor discloses personal data to a processor or third-party controller in accordance with this act, the controller or processor did not have actual knowledge that the processor or third-party controller would violate this act, then the controller or processor may not be considered to have violated this act.

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

(e) Nothing in this act may be construed to do either of the following:

(1) Impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person.

(2) Apply to a person's processing of personal data during the person's personal or household activities.

(f) Personal data processed by a controller pursuant to this section may be processed to the extent that the processing is both of the following:

(1) Reasonably necessary and proportionate to the purposes listed in this section.

(2) Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. The controller or processor must, when applicable, consider the nature and purpose of the collection, use, or retention of the personal data collected, used, or retained pursuant to this section. The personal data must be subject to reasonable administrative, technical, and physical measures to

protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

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

(h) Processing personal data for the purposes expressly identified in this section may not solely make a legal entity a controller with respect to the processing.

Section 11. (a) The Attorney General may enforce violations of this act.

(b)(1) The Attorney General, prior to initiating any action for a violation of any provision of this act, shall issue a notice of violation to the controller.

(2) If the controller fails to correct the violation within 45 days after receipt of the notice of violation, the Attorney General may bring an action for an injunction pursuant to this section. Upon a finding that the controller has violated this act and failed to correct the violation as required by this section, the court may assess a civil penalty of not more than fifteen thousand dollars ($15,000) per violation.

(3) If within the 45-day period the controller corrects the noticed violation and provides the Attorney General an express written statement that the alleged violations have been corrected and that no such further violations will occur,

no action may be initiated against the controller.

Section 12. This act shall become effective on May 1, 2027.

House of Representatives

Read for the first time and referred 29-Jan-26
to the House of Representatives
committee on Commerce and Small
Business

Read for the second time and placed 10-Feb-26
on the calendar:
0 amendments

Read for the third time and passed 24-Feb-26
as amended

Yeas	104
Nays	0
Abs	0

John Treadwell
Clerk