H.B. No. 4

AN ACT

relating to the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities; imposing a civil penalty.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. This Act may be cited as the Texas Data Privacy and Security Act.

SECTION 2. Title 11, Business & Commerce Code, is amended by adding Subtitle C to read as follows:

SUBTITLE C. CONSUMER DATA PROTECTION

CHAPTER 541. CONSUMER DATA PROTECTION

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 541.001. DEFINITIONS. In this chapter, unless a different meaning is required by the context:

(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 subdivision, "control" or "controlled" means:

(A) the ownership of, or power to vote, more than

50 percent of the outstanding shares of any class of voting security of a company;

(B) the control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(C) the 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 Subchapter B is the same consumer exercising those 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. The term includes a fingerprint, voiceprint, eye retina or iris, or other unique biological pattern or characteristic that is used to identify a specific individual. The term does not include a physical or digital photograph or data generated from a physical or digital photograph, a video or audio recording or data generated from a video or audio recording, or 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 by the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).

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

(6) "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 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.

(7) "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.

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

(9) "Covered entity" has the meaning assigned to the term by the Health Insurance Portability and Accountability Act of

1996 (42 U.S.C. Section 1320d et seq.).

(10) "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.

(11) "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.

(12) "Deidentified data" means data that cannot reasonably be linked to an identified or identifiable individual, or a device linked to that individual.

(13) "Health care provider" has the meaning assigned to the term by the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).

(14) "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.

(15) "Identified or identifiable individual" means a consumer who can be readily identified, directly or indirectly.

(16) "Institution of higher education" means:

(A) an institution of higher education as defined by Section 61.003, Education Code; or

(B) a private or independent institution of higher education as defined by Section 61.003, Education Code.

(17) "Known child" means a child under circumstances where a controller has actual knowledge of, or wilfully disregards, the child's age.

(18) "Nonprofit organization" means:

(A) a corporation organized under Chapters 20 and 22, Business Organizations Code, and the provisions of Title 1, Business Organizations Code, to the extent applicable to nonprofit corporations;

(B) an organization exempt from federal taxation

under Section 501(a), Internal Revenue Code of 1986, by being listed as an exempt organization under Section 501(c)(3), 501(c)(6), 501(c)(12), or 501(c)(19) of that code;

(C) a political organization; or

(D) an organization that:

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

(ii) is described by Section 701.052(a), Insurance Code.

(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 deidentified 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 1,750 feet. The term does not include the content of communications or 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 an 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 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 by the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).

(26) "Pseudonymous data" means any information 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 sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include:

(A) the disclosure of personal data to a processor that processes the personal data on the controller's behalf;

(B) the disclosure of personal data to a third party for 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 information that the consumer:

(i) intentionally made available to the general public through a mass media channel; and

(ii) did not restrict to a specific audience; or

(E) the disclosure or transfer of personal data to a third party as an asset that is part of a merger or acquisition.

(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, sexuality, 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 any branch of state government that is created by the constitution or a statute of this state, including a university system or institution of higher education as defined by Section 61.003, Education Code.

(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:

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

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

(iii) is 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.

(33) "Trade secret" means all forms and types of information, including business, scientific, technical, economic, or engineering information, and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and whether or how stored, compiled, or memorialized

physically, electronically, graphically, photographically, or in writing if:

(A) the owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

Sec. 541.002. APPLICABILITY OF CHAPTER. (a) This chapter applies only to a person that:

(1) conducts business in this state or produces a product or service consumed by residents of this state;

(2) processes or engages in the sale of personal data; and

(3) is not a small business as defined by the United States Small Business Administration, except to the extent that Section 541.107 applies to a person described by this subdivision.

(b) This chapter does not apply to:

(1) a state agency or a political subdivision of this state;

(2) a financial institution or data subject to Title V, 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, Title XIII, and Division B, Title IV, Pub. L. No. 111-5);

(4) a nonprofit organization;

(5) an institution of higher education; or

(6) an electric utility, a power generation company, or a retail electric provider, as those terms are defined by Section 31.002, Utilities Code.

Sec. 541.003. CERTAIN INFORMATION EXEMPT FROM CHAPTER. The following information is exempt from this chapter:

(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 chapter 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 deidentified in accordance with the requirements for deidentification under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.);

(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 by the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.) or by a program or a qualified service organization as defined by 42 U.S.C. Section 290dd-2;

(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 by 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 that role;

(16) data processed or maintained as the emergency contact information of an individual under this chapter 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 Subdivision (15) and used for the purposes of administering those benefits.

Sec. 541.004. INAPPLICABILITY OF CHAPTER. This chapter does not apply to the processing of personal data by a person in the course of a purely personal or household activity.

Sec. 541.005. EFFECT OF COMPLIANCE WITH PARENTAL CONSENT REQUIREMENTS UNDER CERTAIN FEDERAL LAW. A controller or processor that complies with the verifiable parental consent requirements of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. Section 6501 et seq.) with respect to data collected online is considered to be in compliance with any requirement to obtain parental consent under this chapter.

SUBCHAPTER B. CONSUMER'S RIGHTS

Sec. 541.051. CONSUMER'S PERSONAL DATA RIGHTS; REQUEST TO EXERCISE RIGHTS. (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, taking into account 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; 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.

Sec. 541.052. CONTROLLER RESPONSE TO CONSUMER REQUEST. (a) Except as otherwise provided by this chapter, a controller shall comply with a request submitted by a consumer to exercise the consumer's rights pursuant to Section 541.051 as provided by this section.

(b) A controller shall respond to the consumer request without undue delay, which may not be later than the 45th day after the date of receipt of the request. The controller may extend the response period once by an additional 45 days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial 45-day response period, together with the reason for the extension.

(c) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, which may not be later than the 45th day 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 541.053.

(d) A controller shall provide information in response to a consumer request free of charge, at least 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 bears 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 is not required to comply with a consumer request submitted under Section 541.051 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 is considered in compliance with a consumer's request to delete that personal data pursuant to Section 541.051(b)(3) 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 chapter; or

(2) opting the consumer out of the processing of that personal data for any purpose other than a purpose that is exempt under the provisions of this chapter.

Sec. 541.053. APPEAL. (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 Section 541.052(c).

(b) The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request under Section 541.051.

(c) A controller shall inform the consumer in writing of any action taken or not taken in response to an appeal under this section not later than the 60th day after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.

(d) If the controller denies an appeal, the controller shall provide the consumer with the online mechanism described by Section 541.152 through which the consumer may contact the attorney general to submit a complaint.

Sec. 541.054. WAIVER OR LIMITATION OF CONSUMER RIGHTS PROHIBITED. Any provision of a contract or agreement that waives or limits in any way a consumer right described by Sections 541.051, 541.052, and 541.053 is contrary to public policy and is void and unenforceable.

Sec. 541.055. METHODS FOR SUBMITTING CONSUMER REQUESTS. (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 chapter. The methods must take into account:

(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 may not require a consumer to create a new account to exercise the consumer's rights under this subchapter but may require a consumer to use an existing account.

(c) Except as provided by Subsection (d), if the controller maintains an Internet website, the controller must provide a mechanism on the website for consumers to submit requests for information required to be disclosed under this chapter.

(d) A controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal information is only required to provide an e-mail address for the submission of requests described by Subsection (c).

(e) A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data under Sections 541.051(b)(5)(A) and (B). A consumer may designate an authorized agent using a technology, including a link to an Internet website, an Internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt out of the processing. A controller shall comply with an opt-out request received from an authorized agent under this subsection if the controller is able to

verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf. A controller is not required to comply with an opt-out request received from an authorized agent under this subsection if:

(1) the authorized agent does not communicate the request to the controller in a clear and unambiguous manner;

(2) the controller is not able to verify, with commercially reasonable effort, that the consumer is a resident of this state;

(3) the controller does not possess the ability to process the request; or

(4) the controller does not process similar or identical requests the controller receives from consumers for the purpose of complying with similar or identical laws or regulations of another state.

(f) A technology described by Subsection (e):

(1) may not unfairly disadvantage another controller;

(2) may not make use of a default setting, but must require the consumer to make an affirmative, freely given, and unambiguous choice to indicate the consumer's intent to opt out of any processing of a consumer's personal data; and

(3) must be consumer-friendly and easy to use by the average consumer.

SUBCHAPTER C. CONTROLLER AND PROCESSOR DATA-RELATED DUTIES AND

PROHIBITIONS

Sec. 541.101. CONTROLLER DUTIES; TRANSPARENCY. (a) A controller:

(1) shall 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, shall 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 may not:

(1) except as otherwise provided by this chapter, 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 of the consumer rights contained in this chapter, 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 (15 U.S.C. Section 6501 et seq.).

(c) Subsection (b)(3) may 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 541.051 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Sec. 541.102. PRIVACY NOTICE. (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 Subchapter B, 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;

(5) if applicable, the categories of third parties with whom the controller shares personal data; and

(6) a description of the methods required under Section 541.055 through which consumers can submit requests to exercise their consumer rights under this chapter.

(b) If a controller engages in the sale of personal data that is sensitive data, the controller shall include the following notice:

"NOTICE: We may sell your sensitive personal data." The notice must be posted in the same location and in the same manner as the privacy notice described by Subsection (a).

(c) If a controller engages in the sale of personal data that is biometric data, the controller shall include the following notice:

"NOTICE: We may sell your biometric personal data." The notice must be posted in the same location and in the same manner as the privacy notice described by Subsection (a).

Sec. 541.103. SALE OF DATA TO THIRD PARTIES AND PROCESSING DATA FOR TARGETED ADVERTISING; DISCLOSURE. If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and

conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process.

Sec. 541.104. DUTIES OF PROCESSOR. (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 chapter, including:

(1) assisting the controller in responding to consumer rights requests submitted under Section 541.051 by using appropriate technical and organizational measures, as reasonably practicable, taking into account the nature of processing and the information available to the processor;

(2) 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 Chapter 521, taking into account the nature of processing and the information available to the processor; and

(3) providing necessary information to enable the controller to conduct and document data protection assessments under Section 541.105.

(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 must 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, on reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with the requirements of this chapter;

(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 Subsection (b)(6)(D), 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 chapter 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) This section may not be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship as described by this chapter.

(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.

Sec. 541.105. DATA PROTECTION ASSESSMENTS. (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) must:

(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:

(A) the use of deidentified data;

(B) the reasonable expectations of consumers;

(C) the context of the processing; and

(D) the relationship between the controller and the consumer whose personal data will be processed.

(c) A controller shall make a data protection assessment requested under Section 541.153(b) available to the attorney general pursuant to a civil investigative demand under Section 541.153.

(d) A data protection assessment is confidential and exempt from public inspection and copying under Chapter 552, Government Code. Disclosure of a data protection assessment in compliance with a request from the attorney general does 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.

Sec. 541.106. DEIDENTIFIED OR PSEUDONYMOUS DATA. (a) A controller in possession of deidentified data shall:

(1) take reasonable measures to ensure that the data cannot be associated with an individual;

(2) publicly commit to maintaining and using deidentified data without attempting to reidentify the data; and

(3) contractually obligate any recipient of the deidentified data to comply with the provisions of this chapter.

(b) This chapter may not be construed to require a controller or processor to:

(1) reidentify deidentified 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 541.051, 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 Sections 541.051(b)(1)-(4) and controller duties under Section 541.101 do 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 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 breach of the contractual commitments.

Sec. 541.107. REQUIREMENTS FOR SMALL BUSINESSES. (a) A person described by Section 541.002(a)(3) may not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer.

(b) A person who violates this section is subject to the penalty under Section 541.155.

SUBCHAPTER D. ENFORCEMENT

Sec. 541.151. ENFORCEMENT AUTHORITY EXCLUSIVE. The attorney general has exclusive authority to enforce this chapter.

Sec. 541.152. INTERNET WEBSITE AND COMPLAINT MECHANISM. The attorney general shall post on the attorney general's Internet website:

(1) information relating to:

(A) the responsibilities of a controller under Subchapters B and C;

(B) the responsibilities of a processor under Subchapter C; and

(C) a consumer's rights under Subchapter B; and

(2) an online mechanism through which a consumer may submit a complaint under this chapter to the attorney general.

Sec. 541.153. INVESTIGATIVE AUTHORITY. (a) If the attorney general has reasonable cause to believe that a person has engaged in or is engaging in a violation of this chapter, the attorney general may issue a civil investigative demand. The procedures established for the issuance of a civil investigative demand under Section 15.10 apply to the same extent and manner to the issuance of a civil investigative demand under this section.

(b) The attorney general may request, pursuant to a civil investigative demand issued under Subsection (a), that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The attorney general may evaluate the data protection assessment for compliance with the requirements set forth in Sections 541.101, 541.102, and 541.103.

Sec. 541.154. NOTICE OF VIOLATION OF CHAPTER; OPPORTUNITY TO CURE. Before bringing an action under Section 541.155, the attorney general shall notify a person in writing, not later than the 30th day before bringing the action, identifying the specific provisions of this chapter the attorney general alleges have been or are being violated. The attorney general may not bring an action

against the person if:

(1) within the 30-day period, the person cures the identified violation; and

(2) the person provides the attorney general a written statement that the person:

(A) cured the alleged violation;

(B) notified the consumer that the consumer's privacy violation was addressed, if the consumer's contact information has been made available to the person;

(C) provided supportive documentation to show how the privacy violation was cured; and

(D) made changes to internal policies, if necessary, to ensure that no such further violations will occur.

Sec. 541.155. CIVIL PENALTY; INJUNCTION. (a) A person who violates this chapter following the cure period described by Section 541.154 or who breaches a written statement provided to the attorney general under that section is liable for a civil penalty in an amount not to exceed $7,500 for each violation.

(b) The attorney general may bring an action in the name of this state to:

(1) recover a civil penalty under this section;

(2) restrain or enjoin the person from violating this chapter; or

(3) recover the civil penalty and seek injunctive relief.

(c) The attorney general may recover reasonable attorney's fees and other reasonable expenses incurred in investigating and bringing an action under this section.

(d) The attorney general shall deposit a civil penalty collected under this section in accordance with Section 402.007, Government Code.

Sec. 541.156. NO PRIVATE RIGHT OF ACTION. This chapter may not be construed as providing a basis for, or being subject to, a private right of action for a violation of this chapter or any other law.

SUBCHAPTER E. CONSTRUCTION OF CHAPTER; EXEMPTIONS FOR CERTAIN USES OF CONSUMER PERSONAL DATA

Sec. 541.201. CONSTRUCTION OF CHAPTER. (a) This chapter may 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) investigate, establish, exercise, prepare for, or defend legal claims;

(4) 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;

(5) 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;

(6) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;

(7) preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security;

(8) 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

(9) assist another controller, processor, or third party with any of the requirements under this subsection.

(b) This chapter may not 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.

(c) This chapter may not be construed as imposing a requirement on controllers and processors that adversely affects the rights or freedoms of any person, including the right of free speech.

(d) This chapter may not be construed as requiring a controller, processor, third party, or consumer to disclose a trade secret.

Sec. 541.202. COLLECTION, USE, OR RETENTION OF DATA FOR CERTAIN PURPOSES. (a) The requirements imposed on controllers and processors under this chapter may 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:

(A) are reasonably aligned with the expectations of the consumer;

(B) are reasonably anticipated based on the consumer's existing relationship with the controller; or

(C) 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.

(b) A requirement imposed on a controller or processor under this chapter does 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.

Sec. 541.203. DISCLOSURE OF PERSONAL DATA TO THIRD-PARTY CONTROLLER OR PROCESSOR. (a) A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this chapter, does not violate this chapter if the third-party controller or processor that receives and processes that personal data is in violation of this chapter, 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 chapter does not violate this chapter for the transgressions of the controller or processor from which the third-party controller or processor receives the personal data.

Sec. 541.204. PROCESSING OF CERTAIN PERSONAL DATA BY

CONTROLLER OR OTHER PERSON. (a) Personal data processed by a controller under this subchapter may not be processed for any purpose other than a purpose listed in this subchapter unless otherwise allowed by this chapter. Personal data processed by a controller under this subchapter may be processed to the extent that the processing of the data is:

(1) reasonably necessary and proportionate to the purposes listed in this subchapter; and

(2) adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this subchapter.

(b) Personal data collected, used, or retained under Section 541.202(a) must, where applicable, take into account 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 this subchapter 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).

(d) The processing of personal data by an entity for the purposes described by Section 541.201 does not solely make the

entity a controller with respect to the processing of the data.

Sec. 541.205. LOCAL PREEMPTION. This chapter supersedes and preempts any ordinance, resolution, rule, or other regulation adopted by a political subdivision regarding the processing of personal data by a controller or processor.

SECTION 3. (a) The Department of Information Resources, under the management of the chief privacy officer, shall review the implementation of the requirements of Chapter 541, Business & Commerce Code, as added by this Act.

(b) Not later than September 1, 2024, the Department of Information Resources shall create an online portal available on the department's Internet website for members of the public to provide feedback and recommend changes to Chapter 541, Business & Commerce Code, as added by this Act. The online portal must remain open for receiving feedback from the public for at least 90 days.

(c) Not later than January 1, 2025, the Department of Information Resources shall make available to the public a report detailing the status of the implementation of the requirements of Chapter 541, Business & Commerce Code, as added by this Act, and any recommendations to the legislature regarding changes to that law.

(d) This section expires September 1, 2025.

SECTION 4. Data protection assessments required to be conducted under Section 541.105, Business & Commerce Code, as added by this Act, apply only to processing activities generated after the effective date of this Act and are not retroactive.

SECTION 5. Not later than July 1, 2024, the attorney general shall post the information and online mechanism required by Section 541.152, Business & Commerce Code, as added by this Act.

SECTION 6. The provisions of this Act are hereby declared severable, and if any provision of this Act or the application of such provision to any person or circumstance is declared invalid for any reason, such declaration shall not affect the validity of the remaining portions of this Act.

SECTION 7. (a) Except as provided by Subsection (b) of this section, this Act takes effect July 1, 2024.

(b) Section 541.055(e), Business & Commerce Code, as added by this Act, takes effect January 1, 2025.

_____ _____

President of the Senate Speaker of the House

I certify that H.B. No. 4 was passed by the House on April 5, 2023, by the following vote: Yeas 146, Nays 0, 1 present, not voting; that the House refused to concur in Senate amendments to H.B. No. 4 on May 15, 2023, and requested the appointment of a conference committee to consider the differences between the two houses; and that the House adopted the conference committee report on H.B. No. 4 on May 28, 2023, by the following vote: Yeas 144,

Nays 0, 1 present, not voting.

_____

Chief Clerk of the House

I certify that H.B. No. 4 was passed by the Senate, with amendments, on May 10, 2023, by the following vote: Yeas 30, Nays 0; at the request of the House, the Senate appointed a conference committee to consider the differences between the two houses; and that the Senate adopted the conference committee report on H.B. No. 4 on May 27, 2023, by the following vote: Yeas 31, Nays 0.

_____

Secretary of the Senate

APPROVED: _____

Date

_____

Governor