

By: Capriglione

H.B. No. 1844

A BILL TO BE ENTITLED

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. 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 SHORT TITLE. This chapter may be cited as the Texas Data Privacy and Security Act.

Sec. 541.002. 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

1           (C) the power to exercise controlling influence  
2 over the management of a company.

3           (2) "Authenticate" means to verify through reasonable  
4 means that the consumer who is entitled to exercise the consumer's  
5 rights under Subchapter B is the same consumer exercising those  
6 consumer rights with respect to the personal data at issue.

7           (3) "Biometric data" "Biometric data" means data  
8 generated by automatic measurements of an individual's biological  
9 characteristics, such as fingerprint, voiceprint, eye retina or  
10 iris, or other unique biological patterns or characteristics, that  
11 are used to identify a specific individual. The term does not  
12 include physical or digital photograph, a video or audio recording,  
13 or data generated therefrom, or information collected, used, or  
14 stored for health care treatment, payment, or operations under the  
15 Health Insurance Portability and Accountability Act of 1996 (42  
16 U.S.C. Section 1320 et seq.)

17           (4) "Business associate" has the meaning assigned to  
18 the term by the Health Insurance Portability and Accountability Act  
19 of 1996 (42 U.S.C. Section 1320d et seq.).

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

22           (6) "Consent," when referring to a consumer, means a  
23 clear affirmative act signifying a consumer's freely given,  
24 specific, informed, and unambiguous agreement to process personal  
25 data relating to the consumer. The term includes a written  
26 statement, including a statement written by electronic means, or  
27 any other unambiguous affirmative action. "Consent" does not

1 include:

2 (A) acceptance of a general or broad terms of use  
3 or similar document that contains descriptions of personal data  
4 processing along with other, unrelated information;

5 (B) hovering over, muting, pausing or closing a  
6 given piece of content; or

7 (C) agreement obtained through the use of dark  
8 patterns.

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

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

16 (9) "Covered entity" has the meaning assigned to the  
17 term by the Health Insurance Portability and Accountability Act of  
18 1996 (42 U.S.C. Section 1320d et seq.).

19 (10) "Dark pattern" means a user interface designed or  
20 manipulated with the substantial effect of subverting or impairing  
21 user autonomy, decision-making or choice, and includes, but is not  
22 limited to, any practice the Federal Trade Commission refers to as a  
23 "dark pattern".

24 (11) "Decision that produces a legal or similarly  
25 significant effect concerning a consumer" means a decision made by  
26 the controller that results in the provision or denial by the  
27 controller of:

- 1           (A) financial and lending services;
- 2           (B) housing, insurance, or health care services;
- 3           (C) education enrollment;
- 4           (D) employment opportunities;
- 5           (E) criminal justice; or
- 6           (F) access to basic necessities, such as food and
- 7 water.

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

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

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

19           (A) the substance of any communication made by an  
20 individual to a health care provider in confidence during or in  
21 connection with the provision of health care services; or

22           (B) information otherwise acquired by the health  
23 care provider about an individual in confidence and in connection  
24 with health care services provided to the individual.

25           (15) "Identified or identifiable individual" means an  
26 individual who can be readily identified, directly or indirectly.

27           (16) "Institution of higher education" means:

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

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

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

8           (18) "Nonprofit organization" means:

9           (A) a corporation organized under Chapters 20 and  
10 22, Business Organizations Code, and the provisions of Title 1,  
11 Business Organizations Code, to the extent applicable to nonprofit  
12 corporations;

13           (B) an organization exempt from federal taxation  
14 under Section 501(a), Internal Revenue Code of 1986, by being  
15 listed as an exempt organization under Section 501(c)(3),  
16 501(c)(6), or 501(c)(12) of that code;

17           (C) a political organization;

18           (D) an organization that:

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

22           (ii) is described by Section 701.052(a),  
23 Insurance Code; or

24           (E) a subsidiary or affiliate of an entity  
25 organized under Chapter 11, Utilities Code.

26           (19) "Personal data" means any information, including  
27 pseudonymous data and sensitive data, that is linked or reasonably

1 linkable to an identified or identifiable individual. The term does  
2 not include deidentified data or publicly available information.

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

7 (A) the selection, nomination, election, or  
8 appointment of an individual to a federal, state, or local public  
9 office or an office in a political organization, regardless of  
10 whether the individual is selected, nominated, elected, or  
11 appointed; or

12 (B) the election of a  
13 presidential/vice-presidential elector, regardless of whether the  
14 elector is selected, nominated, elected, or appointed.

15 (21) "Precise geolocation data" means information  
16 derived from technology, including global positioning system level  
17 latitude and longitude coordinates or other mechanisms, that  
18 directly identifies the specific location of an individual with  
19 precision and accuracy within a radius of 1,750 feet. The term does  
20 not include the content of communications, or any data generated by  
21 or connected to an advanced utility metering infrastructure system  
22 or to equipment for use by a utility.

23 (22) "Process" or "processing" means an operation or  
24 set of operations performed, whether by manual or automated means,  
25 on personal data or on sets of personal data, such as the  
26 collection, use, storage, disclosure, analysis, deletion, or  
27 modification of personal data.

1           (23) "Processor" means a person that processes  
2 personal data on behalf of a controller.

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

8           (25) "Protected health information" has the meaning  
9 assigned to the term by the Health Insurance Portability and  
10 Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).

11           (26) "Pseudonymous data" means personal data that  
12 cannot be attributed to a specific individual without the use of  
13 additional information, provided that the additional information  
14 is kept separately and is subject to appropriate technical and  
15 organizational measures to ensure that the personal data is not  
16 attributed to an identified or identifiable individual.

17           (27) "Publicly available information" means  
18 information that is lawfully made available through government  
19 records, or information that a business has a reasonable basis to  
20 believe is lawfully made available to the general public through  
21 widely distributed media, by a consumer, or by a person to whom a  
22 consumer has disclosed the information, unless the consumer has  
23 restricted the information to a specific audience.

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

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

4           (B) the disclosure of personal data to a third  
5 party for purposes of providing a product or service requested by  
6 the consumer;

7           (C) the disclosure or transfer of personal data  
8 to an affiliate of the controller;

9           (D) the disclosure of information that the  
10 consumer:

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

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

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

17           (29) "Sensitive data" means a category of personal  
18 data. The term includes:

19           (A) personal data revealing racial or ethnic  
20 origin, religious beliefs, mental or physical health diagnosis,  
21 sexual orientation, or citizenship or immigration status;

22           (B) genetic or biometric data that is processed  
23 for the purpose of uniquely identifying an individual;

24           (C) personal data collected from a known child;  
25 or

26           (D) precise geolocation data.

27           (30) "State agency" means a department, commission,



1 board, office, council, authority, or other agency in the executive  
2 branch of state government that is created by the constitution or a  
3 statute of this state, including a university system or institution  
4 of higher education as defined by Section 61.003, Education Code.

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

10 (A) an advertisement that:

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

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

15 (iii) is directed to a consumer in response  
16 to the consumer's request for information or feedback; or

17 (B) the processing of personal data solely for  
18 measuring or reporting advertising performance, reach, or  
19 frequency.

20 (32) "Third party" means a person, other than the  
21 consumer, the controller, the processor, or an affiliate of the  
22 controller or processor.

23 (33) "Trade secret" means all forms and types of  
24 information, including business, scientific, technical, economic,  
25 or engineering information, and any formula, design, prototype,  
26 pattern, plan, compilation, program device, program, code, device,  
27 method, technique, process, procedure, financial data, or list of

1 actual or potential customers or suppliers, whether tangible or  
2 intangible and whether or how stored, compiled, or memorialized  
3 physically, electronically, graphically, photographically, or in  
4 writing if:

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

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

13 Sec. 541.003. APPLICABILITY OF CHAPTER. (a) This chapter  
14 applies only to a person that:

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

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

19 (3) is not a small business as defined by the United  
20 States Small Business Administration.

21 (b) This chapter does not apply to:

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

24 (2) a financial institution or data subject to Title  
25 V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.);

26 (3) a covered entity or business associate governed by  
27 the privacy, security, and breach notification rules issued by the

1 United States Department of Health and Human Services, 45 C.F.R.  
2 Parts 160 and 164, established under the Health Insurance  
3 Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d  
4 et seq.), and the Health Information Technology for Economic and  
5 Clinical Health Act (Division A, Title XIII, and Division B, Title  
6 IV, Pub. L. No. 111-5);

7 (4) a nonprofit organization; or

8 (5) an institution of higher education.

9 Sec. 541.004. CERTAIN INFORMATION EXEMPT FROM CHAPTER. The  
10 following information is exempt from this chapter:

11 (1) protected health information under the Health  
12 Insurance Portability and Accountability Act of 1996 (42 U.S.C.  
13 Section 1320d et seq.);

14 (2) health records;

15 (3) patient identifying information for purposes of 42  
16 U.S.C. Section 290dd-2;

17 (4) identifiable private information:

18 (A) for purposes of the federal policy for the  
19 protection of human subjects under 45 C.F.R. Part 46;

20 (B) collected as part of human subjects research  
21 in accordance with the good clinical practice guidelines issued by  
22 The International Council for Harmonisation of Technical  
23 Requirements for Pharmaceuticals for Human Use (ICH) or of the  
24 protection of human subjects under 21 C.F.R. Parts 6, 50, and 56; or

25 (C) that is personal data used or shared in  
26 research conducted in accordance with the requirements set forth in  
27 this chapter or other research conducted in accordance with

1 applicable law;

2 (5) information and documents created for purposes of  
3 the Health Care Quality Improvement Act of 1986 (42 U.S.C. Section  
4 11101 et seq.);

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

8 (7) information derived from any of the health  
9 care-related information listed in this section that is  
10 deidentified in accordance with the requirements for  
11 deidentification under the Health Insurance Portability and  
12 Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.);

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

20 (9) information collected or used only for public  
21 health activities and purposes as authorized by the Health  
22 Insurance Portability and Accountability Act of 1996 (42 U.S.C.  
23 Section 1320d et seq.);

24 (10) the collection, maintenance, disclosure, sale,  
25 communication, or use of any personal information bearing on a  
26 consumer's creditworthiness, credit standing, credit capacity,  
27 character, general reputation, personal characteristics, or mode

1 of living by a consumer reporting agency or furnisher that provides  
2 information for use in a consumer report, and by a user of a  
3 consumer report, but only to the extent that the activity is  
4 regulated by and authorized under the Fair Credit Reporting Act (15  
5 U.S.C. Section 1681 et seq.);

6 (11) personal data collected, processed, sold, or  
7 disclosed in compliance with the Driver's Privacy Protection Act of  
8 1994 (18 U.S.C. Section 2721 et seq.);

9 (12) personal data regulated by the Family Educational  
10 Rights and Privacy Act of 1974 (20 U.S.C. Section 1232g);

11 (13) personal data collected, processed, sold, or  
12 disclosed in compliance with the Farm Credit Act of 1971 (12 U.S.C.  
13 Section 2001 et seq.);

14 (14) data processed or maintained in the course of an  
15 individual applying to, employed by, or acting as an agent or  
16 independent contractor of a controller, processor, or third party,  
17 to the extent that the data is collected and used within the context  
18 of that role;

19 (15) data processed or maintained as the emergency  
20 contact information of an individual under this chapter that is  
21 used for emergency contact purposes; or

22 (16) data that is processed or maintained and is  
23 necessary to retain to administer benefits for another individual  
24 that relates to an individual described by Subdivision (14) and  
25 used for the purposes of administering those benefits.

26 Sec. 541.005. INAPPLICABILITY OF CHAPTER. This chapter  
27 does not apply to the processing of personal data by a person in the

1 course of a purely personal or household activity.

2 Sec. 541.006. EFFECT OF COMPLIANCE WITH PARENTAL CONSENT  
3 REQUIREMENTS UNDER CERTAIN FEDERAL LAW. A controller or processor  
4 that complies with the verifiable parental consent requirements of  
5 the Children's Online Privacy Protection Act (15 U.S.C. Section  
6 6501 et seq.) with respect to data collected online is considered to  
7 be in compliance with any requirement to obtain parental consent  
8 under this chapter.

9 SUBCHAPTER B. CONSUMER'S RIGHTS

10 Sec. 541.051. CONSUMER'S PERSONAL DATA RIGHTS; REQUEST TO  
11 EXERCISE RIGHTS. (a) A consumer is entitled to exercise the  
12 consumer rights authorized by this section at any time by  
13 submitting a request to a controller specifying the consumer rights  
14 the consumer wishes to exercise. With respect to the processing of  
15 personal data belonging to a known child, a parent or legal guardian  
16 of the child may exercise the consumer rights on behalf of the  
17 child.

18 (b) A controller shall comply with an authenticated  
19 consumer request to exercise the right to:

20 (1) confirm whether a controller is processing the  
21 consumer's personal data and to access the personal data;

22 (2) correct inaccuracies in the consumer's personal  
23 data, taking into account the nature of the personal data and the  
24 purposes of the processing of the consumer's personal data;

25 (3) delete personal data provided by or obtained about  
26 the consumer;

27 (4) if the data is available in a digital format,

1 obtain a copy of the consumer's personal data that the consumer  
2 previously provided to the controller in a portable and, to the  
3 extent technically feasible, readily usable format that allows the  
4 consumer to transmit the data to another controller without  
5 hindrance; or

6 (5) opt out of the processing of the personal data for  
7 purposes of:

8 (A) targeted advertising;

9 (B) the sale of personal data; or

10 (C) profiling in furtherance of a decision that  
11 produces a legal or similarly significant effect concerning the  
12 consumer.

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

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

26 (c) If a controller declines to take action regarding the  
27 consumer's request, the controller shall inform the consumer

1 without undue delay, which may not be later than the 45th day after  
2 the date of receipt of the request, of the justification for  
3 declining to take action and provide instructions on how to appeal  
4 the decision in accordance with Section 541.053.

5 (d) A controller shall provide information in response to a  
6 consumer request free of charge, up to twice annually per consumer.  
7 If a request from a consumer is manifestly unfounded, excessive, or  
8 repetitive, the controller may charge the consumer a reasonable fee  
9 to cover the administrative costs of complying with the request or  
10 may decline to act on the request. The controller bears the burden  
11 of demonstrating for purposes of this subsection that a request is  
12 manifestly unfounded, excessive, or repetitive.

13 (e) If a controller is unable to authenticate the request  
14 using commercially reasonable efforts, the controller is not  
15 required to comply with a consumer request submitted under Section  
16 541.051 and may request that the consumer provide additional  
17 information reasonably necessary to authenticate the consumer and  
18 the consumer's request.

19 (f) A controller that has obtained personal data about a  
20 consumer from a source other than the consumer is considered in  
21 compliance with a consumer's request to delete that personal data  
22 pursuant to Section 541.051(b)(3) by:

23 (1) retaining a record of the deletion request and the  
24 minimum data necessary for the purpose of ensuring the consumer's  
25 personal data remains deleted from the business's records and not  
26 using the retained data for any other purpose under this chapter; or

27 (2) opting the consumer out of the processing of that



1 personal data for any purpose other than a purpose that is exempt  
2 under the provisions of this chapter.

3 Sec. 541.053. APPEAL. (a) A controller shall establish a  
4 process for a consumer to appeal the controller's refusal to take  
5 action on a request within a reasonable period of time after the  
6 consumer's receipt of the decision under Section 541.052(c).

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

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

15 (d) If the controller denies an appeal, the controller shall  
16 provide the consumer with an online mechanism, if available, or  
17 another method through which the consumer may contact the attorney  
18 general to submit a complaint.

19 Sec. 541.054. WAIVER OR LIMITATION OF CONSUMER RIGHTS  
20 PROHIBITED. Any provision of a contract or agreement that waives or  
21 limits in any way a consumer right described by Sections 541.051,  
22 541.052, and 541.053 is contrary to public policy and is void and  
23 unenforceable.

24 Sec. 541.055. METHODS FOR SUBMITTING CONSUMER REQUESTS.

25 (a) A controller shall establish two or more secure and reliable  
26 methods to enable consumers to submit a request to exercise their  
27 consumer rights under this chapter. The methods must take into

1 account:

2 (1) the ways in which consumers normally interact with  
3 the controller;

4 (2) the necessity for secure and reliable  
5 communications of those requests; and

6 (3) the ability of the controller to authenticate the  
7 identity of the consumer making the request.

8 (b) A controller may not require a consumer to create a new  
9 account to exercise the consumer's rights under this subchapter but  
10 may require a consumer to use an existing account.

11 (c) Except as provided by Subsection (d), if the controller  
12 maintains an Internet website, the controller must make the website  
13 available to consumers to submit requests for information required  
14 to be disclosed under this chapter.

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

19 SUBCHAPTER C. CONTROLLER AND PROCESSOR DATA-RELATED DUTIES AND  
20 PROHIBITIONS

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

23 (1) shall limit the collection of personal data to  
24 what is adequate, relevant, and reasonably necessary in relation to  
25 the purposes for which that personal data is processed, as  
26 disclosed to the consumer; and

27 (2) for purposes of protecting the confidentiality,

1 integrity, and accessibility of personal data, shall establish,  
2 implement, and maintain reasonable administrative, technical, and  
3 physical data security practices that are appropriate to the volume  
4 and nature of the personal data at issue.

5 (b) A controller may not:

6 (1) except as otherwise provided by this chapter,  
7 process personal data for a purpose that is neither reasonably  
8 necessary to nor compatible with the disclosed purpose for which  
9 the personal data is processed, as disclosed to the consumer,  
10 unless the controller obtains the consumer's consent;

11 (2) process personal data in violation of state and  
12 federal laws that prohibit unlawful discrimination against  
13 consumers;

14 (3) discriminate against a consumer for exercising any  
15 of the consumer rights contained in this chapter, including by  
16 denying goods or services, charging different prices or rates for  
17 goods or services, or providing a different level of quality of  
18 goods or services to the consumer; or

19 (4) process the sensitive data of a consumer without  
20 obtaining the consumer's consent, or, in the case of processing the  
21 sensitive data of a known child, without processing that data in  
22 accordance with the Children's Online Privacy Protection Act (15  
23 U.S.C. Section 6501 et seq.).

24 (c) Subsection (b)(3) may not be construed to require a  
25 controller to provide a product or service that requires the  
26 personal data of a consumer that the controller does not collect or  
27 maintain or to prohibit a controller from offering a different

1 price, rate, level, quality, or selection of goods or services to a  
2 consumer, including offering goods or services for no fee, if the  
3 consumer has exercised the consumer's right to opt out under  
4 Section 541.051 or the offer is related to a consumer's voluntary  
5 participation in a bona fide loyalty, rewards, premium features,  
6 discounts, or club card program.

7 Sec. 541.102. PRIVACY NOTICE. A controller shall provide  
8 consumers with a reasonably accessible and clear privacy notice  
9 that includes:

10 (1) the categories of personal data processed by the  
11 controller;

12 (a) if applicable, the categories must include  
13 any sensitive data processed by the controller;

14 (2) the purpose for processing personal data;

15 (3) how consumers may exercise their consumer rights  
16 under Subchapter B, including the process by which a consumer may  
17 appeal a controller's decision with regard to the consumer's  
18 request;

19 (4) if applicable, the categories of personal data  
20 that the controller shares with third parties;

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

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

26 Sec. 541.103. SALE OF DATA TO THIRD PARTIES AND PROCESSING  
27 DATA FOR TARGETED ADVERTISING; DISCLOSURE. If a controller sells

1 personal data to third parties or processes personal data for  
2 targeted advertising, the controller shall clearly and  
3 conspicuously disclose such processing and the manner in which a  
4 consumer may exercise the right to opt out of such processing.

5 Sec. 541.104. DUTIES OF PROCESSOR. (a) A processor shall  
6 adhere to the instructions of a controller and shall assist the  
7 controller in meeting or complying with the controller's duties or  
8 requirements under this chapter, including:

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

14 (2) assisting the controller with regard to complying  
15 with the requirement relating to the security of processing  
16 personal data and to the notification of a breach of security of the  
17 processor's system under Chapter 521, taking into account the  
18 nature of processing and the information available to the  
19 processor; and

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

23 (b) A contract between a controller and a processor shall  
24 govern the processor's data processing procedures with respect to  
25 processing performed on behalf of the controller. The contract must  
26 include:

27 (1) clear instructions for processing data;

- 1           (2) the nature and purpose of processing;
- 2           (3) the type of data subject to processing;
- 3           (4) the duration of processing;
- 4           (5) the rights and obligations of both parties; and
- 5           (6) a requirement that the processor shall:

6                   (A) ensure that each person processing personal  
7 data is subject to a duty of confidentiality with respect to the  
8 data;

9                   (B) at the controller's direction, delete or  
10 return all personal data to the controller as requested after the  
11 provision of the service is completed, unless retention of the  
12 personal data is required by law;

13                   (C) make available to the controller, on  
14 reasonable request, all information in the processor's possession  
15 necessary to demonstrate the processor's compliance with the  
16 requirements of this chapter;

17                   (D) allow, and cooperate with, reasonable  
18 assessments by the controller or the controller's designated  
19 assessor; and

20                   (E) engage any subcontractor pursuant to a  
21 written contract that requires the subcontractor to meet the  
22 requirements of the processor with respect to the personal data.

23           (c) Notwithstanding the requirement described by Subsection  
24 (b)(6)(D), a processor, in the alternative, may arrange for a  
25 qualified and independent assessor to conduct an assessment of the  
26 processor's policies and technical and organizational measures in  
27 support of the requirements under this chapter using an appropriate

1 and accepted control standard or framework and assessment  
2 procedure. The processor shall provide a report of the assessment  
3 to the controller on request.

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

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

14 Sec. 541.105. DATA PROTECTION ASSESSMENTS. (a) A  
15 controller shall conduct and document a data protection assessment  
16 of each of the following processing activities involving personal  
17 data:

18 (1) the processing of personal data for purposes of  
19 targeted advertising;

20 (2) the sale of personal data;

21 (3) the processing of personal data for purposes of  
22 profiling, if the profiling presents a reasonably foreseeable risk  
23 of:

24 (A) unfair or deceptive treatment of or unlawful  
25 disparate impact on consumers;

26 (B) financial, physical, or reputational injury  
27 to consumers;

1           (C) a physical or other intrusion on the solitude  
2 or seclusion, or the private affairs or concerns, of consumers, if  
3 the intrusion would be offensive to a reasonable person; or

4           (D) other substantial injury to consumers;

5           (4) the processing of sensitive data; and

6           (5) any processing activities involving personal data  
7 that present a heightened risk of harm to consumers.

8           (b) A data protection assessment conducted under Subsection  
9 (a) must:

10           (1) identify and weigh the direct or indirect benefits  
11 that may flow from the processing to the controller, the consumer,  
12 other stakeholders, and the public, against the potential risks to  
13 the rights of the consumer associated with that processing, as  
14 mitigated by safeguards that can be employed by the controller to  
15 reduce the risks; and

16           (2) factor into the assessment:

17                   (A) the use of deidentified data;

18                   (B) the reasonable expectations of consumers;

19                   (C) the context of the processing; and

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

22           (c) A controller shall make a data protection assessment  
23 requested under Section 541.152(b) available to the attorney  
24 general.

25           (d) A data protection assessment is confidential and exempt  
26 from public inspection and copying under Chapter 552, Government  
27 Code. Disclosure of a data protection assessment in compliance with



1 a request from the attorney general does not constitute a waiver of  
2 attorney-client privilege or work product protection with respect  
3 to the assessment and any information contained in the assessment.

4 (e) A single data protection assessment may address a  
5 comparable set of processing operations that include similar  
6 activities.

7 (f) A data protection assessment conducted by a controller  
8 for the purpose of compliance with other laws or regulations may  
9 constitute compliance with the requirements of this section if the  
10 assessment has a reasonably comparable scope and effect.

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

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

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

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

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

21 (1) reidentify deidentified data or pseudonymous  
22 data;

23 (2) maintain data in identifiable form or obtain,  
24 retain, or access any data or technology for the purpose of allowing  
25 the controller or processor to associate a consumer request with  
26 personal data; or

27 (3) comply with an authenticated consumer rights

1 request under Section 541.051, if the controller:

2 (A) is not reasonably capable of associating the  
3 request with the personal data or it would be unreasonably  
4 burdensome for the controller to associate the request with the  
5 personal data;

6 (B) does not use the personal data to recognize  
7 or respond to the specific consumer who is the subject of the  
8 personal data or associate the personal data with other personal  
9 data about the same specific consumer; and

10 (C) does not sell the personal data to any third  
11 party or otherwise voluntarily disclose the personal data to any  
12 third party other than a processor, except as otherwise permitted  
13 by this section.

14 (c) The consumer rights under Sections 541.051(b)(1)-(4)  
15 and controller duties under Section 541.101 do not apply to  
16 pseudonymous data in cases in which the controller is able to  
17 demonstrate any information necessary to identify the consumer is  
18 kept separately and is subject to effective technical and  
19 organizational controls that prevent the controller from accessing  
20 the information.

21 (d) A controller that discloses pseudonymous data or  
22 deidentified data shall exercise reasonable oversight to monitor  
23 compliance with any contractual commitments to which the  
24 pseudonymous data or deidentified data is subject and shall take  
25 appropriate steps to address any breach of the contractual  
26 commitments.

SUBCHAPTER D. ENFORCEMENT

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

Sec. 541.152. INVESTIGATIVE AUTHORITY. (a) If the attorney general has reasonable cause to believe that a person has engaged in, is engaging in, or is about to engage 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. 541.153. NOTICE OF VIOLATION OF CHAPTER; OPPORTUNITY TO CURE. Before bringing an action under Section 541.154, 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

1           (2) the person provides the attorney general a written  
2 statement that the alleged violation has been cured and that no  
3 further violations will occur.

4           Sec. 541.154. CIVIL PENALTY; INJUNCTION. (a) A person who  
5 violates this chapter following the cure period described by  
6 Section 541.153 or who breaches a written statement provided to the  
7 attorney general under that section is liable for a civil penalty in  
8 an amount not to exceed \$7,500 for each violation.

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

11               (1) recover a civil penalty under this section;

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

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

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

19           (d) The attorney general shall deposit a civil penalty  
20 collected under this section in the state treasury to the credit of  
21 the general revenue fund.

22           Sec. 541.155. NO PRIVATE RIGHT OF ACTION. This chapter may  
23 not be construed to create a private right of action for a violation  
24 of this chapter or any other chapter.

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

27           Sec. 541.201. CONSTRUCTION OF CHAPTER. (a) This chapter

1 may not be construed to restrict a controller's or processor's  
2 ability to:

3 (1) comply with federal, state, or local laws, rules,  
4 or regulations;

5 (2) comply with a civil, criminal, or regulatory  
6 inquiry, investigation, subpoena, or summons by federal, state,  
7 local, or other governmental authorities;

8 (3) investigate, establish, exercise, prepare for, or  
9 defend legal claims;

10 (4) provide a product or service specifically  
11 requested by a consumer or the parent or guardian of a child,  
12 perform a contract to which the consumer is a party, including  
13 fulfilling the terms of a written warranty, or take steps at the  
14 request of the consumer before entering into a contract;

15 (5) take immediate steps to protect an interest that  
16 is essential for the life or physical safety of the consumer or of  
17 another individual and in which the processing cannot be manifestly  
18 based on another legal basis;

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

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

25 (8) engage in public or peer-reviewed scientific or  
26 statistical research in the public interest that adheres to all  
27 other applicable ethics and privacy laws and is approved,

1 monitored, and governed by an institutional review board or similar  
2 independent oversight entity that determines:

3 (A) if the deletion of the information is likely  
4 to provide substantial benefits that do not exclusively accrue to  
5 the controller;

6 (B) whether the expected benefits of the research  
7 outweigh the privacy risks; and

8 (C) if the controller has implemented reasonable  
9 safeguards to mitigate privacy risks associated with research,  
10 including any risks associated with reidentification; or

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

13 (b) This chapter may not be construed to prevent a  
14 controller or processor from providing personal data concerning a  
15 consumer to a person covered by an evidentiary privilege under the  
16 laws of this state as part of a privileged communication.

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

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

24 Sec. 541.202. COLLECTION, USE, OR RETENTION OF DATA FOR  
25 CERTAIN PURPOSES. (a) The requirements imposed on controllers and  
26 processors under this chapter may not restrict a controller's or  
27 processor's ability to collect, use, or retain data to:

1           (1) conduct internal research to develop, improve, or  
2 repair products, services, or technology;

3           (2) effect a product recall;

4           (3) identify and repair technical errors that impair  
5 existing or intended functionality; or

6           (4) perform internal operations that:

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

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

11           (C) are otherwise compatible with processing  
12 data in furtherance of the provision of a product or service  
13 specifically requested by a consumer or the performance of a  
14 contract to which the consumer is a party.

15           (b) A requirement imposed on a controller or processor under  
16 this chapter does not apply if compliance with the requirement by  
17 the controller or processor, as applicable, would violate an  
18 evidentiary privilege under the laws of this state.

19           Sec. 541.203. DISCLOSURE OF PERSONAL DATA TO THIRD-PARTY  
20 CONTROLLER OR PROCESSOR. (a) A controller or processor that  
21 discloses personal data to a third-party controller or processor,  
22 in compliance with the requirements of this chapter, does not  
23 violate this chapter if the third-party controller or processor  
24 that receives and processes that personal data is in violation of  
25 this chapter, provided that, at the time of the data's disclosure,  
26 the disclosing controller or processor did not have actual  
27 knowledge that the recipient intended to commit a violation.

1       (b) A third-party controller or processor receiving  
2 personal data from a controller or processor in compliance with the  
3 requirements of this chapter does not violate this chapter for the  
4 transgressions of the controller or processor from which the  
5 third-party controller or processor receives the personal data.

6       Sec. 541.204. PROCESSING OF CERTAIN PERSONAL DATA BY  
7 CONTROLLER OR OTHER PERSON. (a) Personal data processed by a  
8 controller under this subchapter may not be processed for any  
9 purpose other than a purpose listed in this subchapter unless  
10 otherwise allowed by this chapter. Personal data processed by a  
11 controller under this subchapter may be processed to the extent  
12 that the processing of the data is:

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

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

18       (b) Personal data collected, used, or retained under  
19 Section 541.202(a) must, where applicable, take into account the  
20 nature and purpose of such collection, use, or retention. The  
21 personal data described by this subsection is subject to reasonable  
22 administrative, technical, and physical measures to protect the  
23 confidentiality, integrity, and accessibility of the personal data  
24 and to reduce reasonably foreseeable risks of harm to consumers  
25 relating to the collection, use, or retention of personal data.

26       (c) A controller that processes personal data under an  
27 exemption in this subchapter bears the burden of demonstrating that



1 the processing of the personal data qualifies for the exemption and  
2 complies with the requirements of Subsections (a) and (b).

3 (d) The processing of personal data by an entity for the  
4 purposes described by Section 541.201 does not solely make the  
5 entity a controller with respect to the processing of the data.

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

10 SECTION 2. (a) The Department of Information Resources,  
11 under the management of the chief privacy officer, shall review the  
12 implementation of the requirements of Chapter 541, Business &  
13 Commerce Code, as added by this Act.

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

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

25 (d) This section expires September 1, 2025.

26 SECTION 3. The provisions of this Act are hereby declared  
27 severable, and if any provision of this Act or the application of

1 such provision to any person or circumstance is declared invalid  
2 for any reason, such declaration shall not affect the validity of  
3 the remaining portions of this Act.

4 SECTION 4. This Act takes effect September 1, 2023.