

1 AN ACT

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

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

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

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

10 SUBTITLE C. CONSUMER DATA PROTECTION

11 CHAPTER 541. CONSUMER DATA PROTECTION

12 SUBCHAPTER A. GENERAL PROVISIONS

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

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

19 (A) the ownership of, or power to vote, more than
20 50 percent of the outstanding shares of any class of voting security
21 of a company;

22 (B) the control in any manner over the election
23 of a majority of the directors or of individuals exercising similar
24 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" means data generated by automatic
8 measurements of an individual's biological characteristics. The
9 term includes a fingerprint, voiceprint, eye retina or iris, or
10 other unique biological pattern or characteristic that is used to
11 identify a specific individual. The term does not include a
12 physical or digital photograph or data generated from a physical or
13 digital photograph, a video or audio recording or data generated
14 from a video or audio recording, or information collected, used, or
15 stored for health care treatment, payment, or operations under the
16 Health Insurance Portability and Accountability Act of 1996 (42
17 U.S.C. Section 1320d et seq.).

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

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

23 (6) "Consent," when referring to a consumer, means a
24 clear affirmative act signifying a consumer's freely given,
25 specific, informed, and unambiguous agreement to process personal
26 data relating to the consumer. The term includes a written
27 statement, including a statement written by electronic means, or

1 any other unambiguous affirmative action. The term does not
2 include:

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

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

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

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

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

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

20 (10) "Dark pattern" means a user interface designed or
21 manipulated with the effect of substantially subverting or
22 impairing user autonomy, decision-making, or choice, and includes
23 any practice the Federal Trade Commission refers to as a dark
24 pattern.

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

1 controller of:

2 (A) financial and lending services;

3 (B) housing, insurance, or health care services;

4 (C) education enrollment;

5 (D) employment opportunities;

6 (E) criminal justice; or

7 (F) access to basic necessities, such as food and
8 water.

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

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

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

19 The term includes:

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

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

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

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

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

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

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

9 (18) "Nonprofit organization" means:

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

14 (B) an organization exempt from federal taxation
15 under Section 501(a), Internal Revenue Code of 1986, by being
16 listed as an exempt organization under Section 501(c)(3),
17 501(c)(6), 501(c)(12), or 501(c)(19) of that code;

18 (C) a political organization; or

19 (D) an organization that:

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

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

25 (19) "Personal data" means any information, including
26 sensitive data, that is linked or reasonably linkable to an
27 identified or identifiable individual. The term includes

1 pseudonymous data when the data is used by a controller or processor
2 in conjunction with additional information that reasonably links
3 the data to an identified or identifiable individual. The term does
4 not include deidentified data or publicly available information.

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

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

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

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

25 (22) "Process" or "processing" means an operation or
26 set of operations performed, whether by manual or automated means,
27 on personal data or on sets of personal data, such as the

1 collection, use, storage, disclosure, analysis, deletion, or
2 modification of personal data.

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

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

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

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

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

26 (28) "Sale of personal data" means the sharing,
27 disclosing, or transferring of personal data for monetary or other

1 valuable consideration by the controller to a third party. The term
2 does not include:

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

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

9 (C) the disclosure or transfer of personal data
10 to an affiliate of the controller;

11 (D) the disclosure of information that the
12 consumer:

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

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

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

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

21 (A) personal data revealing racial or ethnic
22 origin, religious beliefs, mental or physical health diagnosis,
23 sexuality, or citizenship or immigration status;

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

26 (C) personal data collected from a known child;

27 or

1 (D) precise geolocation data.

2 (30) "State agency" means a department, commission,
3 board, office, council, authority, or other agency in any branch of
4 state government that is created by the constitution or a statute of
5 this state, including a university system or institution of higher
6 education as defined by Section 61.003, Education Code.

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

12 (A) an advertisement that:

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

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

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

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

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

25 (33) "Trade secret" means all forms and types of
26 information, including business, scientific, technical, economic,
27 or engineering information, and any formula, design, prototype,

1 pattern, plan, compilation, program device, program, code, device,
2 method, technique, process, procedure, financial data, or list of
3 actual or potential customers or suppliers, whether tangible or
4 intangible and whether or how stored, compiled, or memorialized
5 physically, electronically, graphically, photographically, or in
6 writing if:

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

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

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

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

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

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

24 (b) This chapter does not apply to:

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

27 (2) a financial institution or data subject to Title

1 V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.);

2 (3) a covered entity or business associate governed by
3 the privacy, security, and breach notification rules issued by the
4 United States Department of Health and Human Services, 45 C.F.R.
5 Parts 160 and 164, established under the Health Insurance
6 Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d
7 et seq.), and the Health Information Technology for Economic and
8 Clinical Health Act (Division A, Title XIII, and Division B, Title
9 IV, Pub. L. No. 111-5);

10 (4) a nonprofit organization;

11 (5) an institution of higher education; or

12 (6) an electric utility, a power generation company,
13 or a retail electric provider, as those terms are defined by Section
14 31.002, Utilities Code.

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

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

20 (2) health records;

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

23 (4) identifiable private information:

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

26 (B) collected as part of human subjects research
27 under the good clinical practice guidelines issued by The

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

4 (C) that is personal data used or shared in
5 research conducted in accordance with the requirements set forth in
6 this chapter or other research conducted in accordance with
7 applicable law;

8 (5) information and documents created for purposes of
9 the Health Care Quality Improvement Act of 1986 (42 U.S.C. Section
10 11101 et seq.);

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

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

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

26 (9) information that is included in a limited data set
27 as described by 45 C.F.R. Section 164.514(e), to the extent that the

1 information is used, disclosed, and maintained in the manner
2 specified by 45 C.F.R. Section 164.514(e);

3 (10) information collected or used only for public
4 health activities and purposes as authorized by the Health
5 Insurance Portability and Accountability Act of 1996 (42 U.S.C.
6 Section 1320d et seq.);

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

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

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

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

24 (15) data processed or maintained in the course of an
25 individual applying to, being employed by, or acting as an agent or
26 independent contractor of a controller, processor, or third party,
27 to the extent that the data is collected and used within the context

1 of that role;

2 (16) data processed or maintained as the emergency
3 contact information of an individual under this chapter that is
4 used for emergency contact purposes; or

5 (17) data that is processed or maintained and is
6 necessary to retain to administer benefits for another individual
7 that relates to an individual described by Subdivision (15) and
8 used for the purposes of administering those benefits.

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

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

19 SUBCHAPTER B. CONSUMER'S RIGHTS

20 Sec. 541.051. CONSUMER'S PERSONAL DATA RIGHTS; REQUEST TO
21 EXERCISE RIGHTS. (a) A consumer is entitled to exercise the
22 consumer rights authorized by this section at any time by
23 submitting a request to a controller specifying the consumer rights
24 the consumer wishes to exercise. With respect to the processing of
25 personal data belonging to a known child, a parent or legal guardian
26 of the child may exercise the consumer rights on behalf of the
27 child.

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

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

5 (2) correct inaccuracies in the consumer's personal
6 data, taking into account the nature of the personal data and the
7 purposes of the processing of the consumer's personal data;

8 (3) delete personal data provided by or obtained about
9 the consumer;

10 (4) if the data is available in a digital format,
11 obtain a copy of the consumer's personal data that the consumer
12 previously provided to the controller in a portable and, to the
13 extent technically feasible, readily usable format that allows the
14 consumer to transmit the data to another controller without
15 hindrance; or

16 (5) opt out of the processing of the personal data for
17 purposes of:

18 (A) targeted advertising;

19 (B) the sale of personal data; or

20 (C) profiling in furtherance of a decision that
21 produces a legal or similarly significant effect concerning the
22 consumer.

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

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

9 (c) If a controller declines to take action regarding the
10 consumer's request, the controller shall inform the consumer
11 without undue delay, which may not be later than the 45th day after
12 the date of receipt of the request, of the justification for
13 declining to take action and provide instructions on how to appeal
14 the decision in accordance with Section 541.053.

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

23 (e) If a controller is unable to authenticate the request
24 using commercially reasonable efforts, the controller is not
25 required to comply with a consumer request submitted under Section
26 541.051 and may request that the consumer provide additional
27 information reasonably necessary to authenticate the consumer and

1 the consumer's request.

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

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

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

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

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

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

25 (d) If the controller denies an appeal, the controller shall
26 provide the consumer with the online mechanism described by Section
27 541.152 through which the consumer may contact the attorney general

1 to submit a complaint.

2 Sec. 541.054. WAIVER OR LIMITATION OF CONSUMER RIGHTS
3 PROHIBITED. Any provision of a contract or agreement that waives or
4 limits in any way a consumer right described by Sections 541.051,
5 541.052, and 541.053 is contrary to public policy and is void and
6 unenforceable.

7 Sec. 541.055. METHODS FOR SUBMITTING CONSUMER REQUESTS.

8 (a) A controller shall establish two or more secure and reliable
9 methods to enable consumers to submit a request to exercise their
10 consumer rights under this chapter. The methods must take into
11 account:

12 (1) the ways in which consumers normally interact with
13 the controller;

14 (2) the necessity for secure and reliable
15 communications of those requests; and

16 (3) the ability of the controller to authenticate the
17 identity of the consumer making the request.

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

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

25 (d) A controller that operates exclusively online and has a
26 direct relationship with a consumer from whom the controller
27 collects personal information is only required to provide an e-mail

1 address for the submission of requests described by Subsection (c).

2 (e) A consumer may designate another person to serve as the
3 consumer's authorized agent and act on the consumer's behalf to opt
4 out of the processing of the consumer's personal data under
5 Sections 541.051(b)(5)(A) and (B). A consumer may designate an
6 authorized agent using a technology, including a link to an
7 Internet website, an Internet browser setting or extension, or a
8 global setting on an electronic device, that allows the consumer to
9 indicate the consumer's intent to opt out of the processing. A
10 controller shall comply with an opt-out request received from an
11 authorized agent under this subsection if the controller is able to
12 verify, with commercially reasonable effort, the identity of the
13 consumer and the authorized agent's authority to act on the
14 consumer's behalf. A controller is not required to comply with an
15 opt-out request received from an authorized agent under this
16 subsection if:

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

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

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

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

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

2 (1) may not unfairly disadvantage another controller;

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

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

9 SUBCHAPTER C. CONTROLLER AND PROCESSOR DATA-RELATED DUTIES AND
10 PROHIBITIONS

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

13 (1) shall limit the collection of personal data to
14 what is adequate, relevant, and reasonably necessary in relation to
15 the purposes for which that personal data is processed, as
16 disclosed to the consumer; and

17 (2) for purposes of protecting the confidentiality,
18 integrity, and accessibility of personal data, shall establish,
19 implement, and maintain reasonable administrative, technical, and
20 physical data security practices that are appropriate to the volume
21 and nature of the personal data at issue.

22 (b) A controller may not:

23 (1) except as otherwise provided by this chapter,
24 process personal data for a purpose that is neither reasonably
25 necessary to nor compatible with the disclosed purpose for which
26 the personal data is processed, as disclosed to the consumer,
27 unless the controller obtains the consumer's consent;

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

4 (3) discriminate against a consumer for exercising any
5 of the consumer rights contained in this chapter, including by
6 denying goods or services, charging different prices or rates for
7 goods or services, or providing a different level of quality of
8 goods or services to the consumer; or

9 (4) process the sensitive data of a consumer without
10 obtaining the consumer's consent, or, in the case of processing the
11 sensitive data of a known child, without processing that data in
12 accordance with the Children's Online Privacy Protection Act of
13 1998 (15 U.S.C. Section 6501 et seq.).

14 (c) Subsection (b)(3) may not be construed to require a
15 controller to provide a product or service that requires the
16 personal data of a consumer that the controller does not collect or
17 maintain or to prohibit a controller from offering a different
18 price, rate, level, quality, or selection of goods or services to a
19 consumer, including offering goods or services for no fee, if the
20 consumer has exercised the consumer's right to opt out under
21 Section 541.051 or the offer is related to a consumer's voluntary
22 participation in a bona fide loyalty, rewards, premium features,
23 discounts, or club card program.

24 Sec. 541.102. PRIVACY NOTICE. (a) A controller shall
25 provide consumers with a reasonably accessible and clear privacy
26 notice that includes:

27 (1) the categories of personal data processed by the

1 controller, including, if applicable, any sensitive data processed
2 by the controller;

3 (2) the purpose for processing personal data;

4 (3) how consumers may exercise their consumer rights
5 under Subchapter B, including the process by which a consumer may
6 appeal a controller's decision with regard to the consumer's
7 request;

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

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

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

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

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

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

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

27 Sec. 541.103. SALE OF DATA TO THIRD PARTIES AND PROCESSING

1 DATA FOR TARGETED ADVERTISING; DISCLOSURE. If a controller sells
2 personal data to third parties or processes personal data for
3 targeted advertising, the controller shall clearly and
4 conspicuously disclose that process and the manner in which a
5 consumer may exercise the right to opt out of that process.

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

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

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

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

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

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

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

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

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

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

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

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

1 support of the requirements under this chapter using an appropriate
2 and accepted control standard or framework and assessment
3 procedure. The processor shall provide a report of the assessment
4 to the controller on request.

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

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

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

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

21 (2) the sale of personal data;

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

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

27 (B) financial, physical, or reputational injury

1 to consumers;

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

5 (D) other substantial injury to consumers;

6 (4) the processing of sensitive data; and

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

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

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

17 (2) factor into the assessment:

18 (A) the use of deidentified data;

19 (B) the reasonable expectations of consumers;

20 (C) the context of the processing; and

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

23 (c) A controller shall make a data protection assessment
24 requested under Section 541.153(b) available to the attorney
25 general pursuant to a civil investigative demand under Section
26 541.153.

27 (d) A data protection assessment is confidential and exempt

1 from public inspection and copying under Chapter 552, Government
2 Code. Disclosure of a data protection assessment in compliance with
3 a request from the attorney general does not constitute a waiver of
4 attorney-client privilege or work product protection with respect
5 to the assessment and any information contained in the assessment.

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

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

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

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

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

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

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

23 (1) reidentify deidentified data or pseudonymous
24 data;

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

1 personal data; or

2 (3) comply with an authenticated consumer rights
3 request under Section 541.051, if the controller:

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

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

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

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

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

1 commitments.

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

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

8 SUBCHAPTER D. ENFORCEMENT

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

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

14 (1) information relating to:

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

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

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

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

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

1 the issuance of a civil investigative demand under this section.

2 (b) The attorney general may request, pursuant to a civil
3 investigative demand issued under Subsection (a), that a controller
4 disclose any data protection assessment that is relevant to an
5 investigation conducted by the attorney general. The attorney
6 general may evaluate the data protection assessment for compliance
7 with the requirements set forth in Sections 541.101, 541.102, and
8 541.103.

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

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

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

20 (A) cured the alleged violation;

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

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

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

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

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

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

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

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

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

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

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

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

25 Sec. 541.201. CONSTRUCTION OF CHAPTER. (a) This chapter
26 may not be construed to restrict a controller's or processor's
27 ability to:

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

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

6 (3) investigate, establish, exercise, prepare for, or
7 defend legal claims;

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

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

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

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

23 (8) engage in public or peer-reviewed scientific or
24 statistical research in the public interest that adheres to all
25 other applicable ethics and privacy laws and is approved,
26 monitored, and governed by an institutional review board or similar
27 independent oversight entity that determines:

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

4 (B) whether the expected benefits of the research
5 outweigh the privacy risks; and

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

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

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

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

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

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

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

1 (2) effect a product recall;

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

4 (4) perform internal operations that:

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

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

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

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

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

26 (b) A third-party controller or processor receiving
27 personal data from a controller or processor in compliance with the

1 requirements of this chapter does not violate this chapter for the
2 transgressions of the controller or processor from which the
3 third-party controller or processor receives the personal data.

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

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

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

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

24 (c) A controller that processes personal data under an
25 exemption in this subchapter bears the burden of demonstrating that
26 the processing of the personal data qualifies for the exemption and
27 complies with the requirements of Subsections (a) and (b).

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

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

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

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

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

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

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

1 SECTION 5. Not later than July 1, 2024, the attorney general
2 shall post the information and online mechanism required by Section
3 541.152, Business & Commerce Code, as added by this Act.

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

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

11 (b) Section 541.055(e), Business & Commerce Code, as added
12 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

H.B. No. 4

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