## **SENATE AMENDMENTS**

## 2<sup>nd</sup> Printing

By: Capriglione, Longoria, Burrows, Meyer, H.B. No. 4 et al.

## A BILL TO BE ENTITLED

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, a video or audio recording or data
- 13 generated from a video or audio recording, or information
- 14 collected, used, or stored for health care treatment, payment, or
- 15 operations under the Health Insurance Portability and
- 16 Accountability Act of 1996 (42 U.S.C. Section 1320d 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 <u>of age.</u>
- 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. The term does not

- 1 <u>include:</u>
- 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 effect of substantially subverting or
- 21 <u>impairing user autonomy, decision-making, or choice, and includes</u>
- 22 any practice the Federal Trade Commission refers to as a dark
- 23 pattern.
- 24 (11) "Decision that produces a legal or similarly
- 25 <u>significant effect concerning a consumer" means a decision made by</u>
- 26 the controller that results in the provision or denial by the
- 27 controller of:

Η	R	No.	Δ

	11.2. 110.
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 a
26	consumer 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 wilfully disregards,
7	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	regulated under Subtitle B, Title 2, Utilities Code.
26	(19) "Personal data" means any information, including
27	sensitive data, that is linked or reasonably linkable to an

```
H.B. No. 4
```

- 1 identified or identifiable individual. The term includes
- 2 pseudonymous data when the data is used by a controller or processor
- 3 in conjunction with additional information that reasonably links
- 4 the data to an identified or identifiable individual. The term does
- 5 not include deidentified data or publicly available information.
- 6 (20) "Political organization" means a party,
- 7 committee, association, fund, or other organization, regardless of
- 8 whether incorporated, that is organized and operated primarily for
- 9 the purpose of influencing or attempting to influence:
- 10 (A) the selection, nomination, election, or
- 11 appointment of an individual to a federal, state, or local public
- 12 office or an office in a political organization, regardless of
- 13 whether the individual is selected, nominated, elected, or
- 14 appointed; or
- 15 (B) the election of a
- 16 presidential/vice-presidential elector, regardless of whether the
- 17 <u>elector is selected</u>, nominated, elected, or appointed.
- 18 (21) "Precise geolocation data" means information
- 19 derived from technology, including global positioning system level
- 20 latitude and longitude coordinates or other mechanisms, that
- 21 directly identifies the specific location of an individual with
- 22 precision and accuracy within a radius of 1,750 feet. The term does
- 23 not include the content of communications or any data generated by
- 24 or connected to an advanced utility metering infrastructure system
- 25 or to equipment for use by a utility.
- 26 (22) "Process" or "processing" means an operation or
- 27 set of operations performed, whether by manual or automated means,

H.B. No. 4

- 1 on personal data or on sets of personal data, such as the
- 2 collection, use, storage, disclosure, analysis, deletion, or
- 3 modification of personal data.
- 4 (23) "Processor" means a person that processes
- 5 personal data on behalf of a controller.
- 6 (24) "Profiling" means any form of solely automated
- 7 processing performed on personal data to evaluate, analyze, or
- 8 predict personal aspects related to an identified or identifiable
- 9 individual's economic situation, health, personal preferences,
- 10 interests, reliability, behavior, location, or movements.
- 11 (25) "Protected health information" has the meaning
- 12 assigned to the term by the Health Insurance Portability and
- 13 Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).
- 14 (26) "Pseudonymous data" means any information that
- 15 cannot be attributed to a specific individual without the use of
- 16 additional information, provided that the additional information
- 17 is kept separately and is subject to appropriate technical and
- 18 organizational measures to ensure that the personal data is not
- 19 attributed to an identified or identifiable individual.
- 20 (27) "Publicly available information" means
- 21 information that is lawfully made available through government
- 22 records, or information that a business has a reasonable basis to
- 23 believe is lawfully made available to the general public through
- 24 widely distributed media, by a consumer, or by a person to whom a
- 25 consumer has disclosed the information, unless the consumer has
- 26 restricted the information to a specific audience.
- 27 (28) "Sale of personal data" means the sharing,

- 1 disclosing, or transferring of personal data for monetary or other
- 2 valuable consideration by the controller to a third party. The term
- 3 does not include:
- 4 (A) the disclosure of personal data to a
- 5 processor that processes the personal data on the controller's
- 6 behalf;
- 7 (B) the disclosure of personal data to a third
- 8 party for purposes of providing a product or service requested by
- 9 the consumer;
- 10 <u>(C) the disclosure or transfer of personal data</u>
- 11 to an affiliate of the controller;
- 12 (D) the disclosure of information that the
- 13 <u>consumer:</u>
- 14 (i) intentionally made available to the
- 15 general public through a mass media channel; and
- (ii) did not restrict to a specific
- 17 audience; or
- 18 (E) the disclosure or transfer of personal data
- 19 to a third party as an asset that is part of a merger or acquisition.
- 20 (29) "Sensitive data" means a category of personal
- 21 data. The term includes:
- (A) personal data revealing racial or ethnic
- 23 origin, religious beliefs, mental or physical health diagnosis,
- 24 sexual orientation, or citizenship or immigration status;
- 25 (B) genetic or biometric data that is processed
- 26 for the purpose of uniquely identifying an individual;
- (C) personal data collected from a known child;

1	<u>or</u>
2	(D) precise geolocation data.
3	(30) "State agency" means a department, commission,
4	board, office, council, authority, or other agency in the executive
5	branch of state government that is created by the constitution or a
6	statute of this state, including a university system or institution
7	of higher education as defined by Section 61.003, Education Code.
8	(31) "Targeted advertising" means displaying to a
9	consumer an advertisement that is selected based on personal data
10	obtained from that consumer's activities over time and across
11	nonaffiliated websites or online applications to predict the
12	consumer's preferences or interests. The term does not include:
13	(A) an advertisement that:
14	(i) is based on activities within a
15	controller's own websites or online applications;
16	(ii) is based on the context of a consumer's
17	current search query, visit to a website, or online application; or
18	(iii) is directed to a consumer in response
19	to the consumer's request for information or feedback; or
20	(B) the processing of personal data solely for
21	measuring or reporting advertising performance, reach, or
22	frequency.
23	(32) "Third party" means a person, other than the
24	consumer, the controller, the processor, or an affiliate of the
25	controller or processor.
26	(33) "Trade secret" means all forms and types of
27	information, including business, scientific, technical, economic,

- 1 or engineering information, and any formula, design, prototype,
- 2 pattern, plan, compilation, program device, program, code, device,
- 3 method, technique, process, procedure, financial data, or list of
- 4 actual or potential customers or suppliers, whether tangible or
- 5 intangible and whether or how stored, compiled, or memorialized
- 6 physically, electronically, graphically, photographically, or in
- 7 writing if:
- 8 (A) the owner of the trade secret has taken
- 9 reasonable measures under the circumstances to keep the information
- 10 secret; and
- 11 (B) the information derives independent economic
- 12 value, actual or potential, from not being generally known to, and
- 13 not being readily ascertainable through proper means by, another
- 14 person who can obtain economic value from the disclosure or use of
- 15 the information.
- Sec. 541.002. APPLICABILITY OF CHAPTER. (a) This chapter
- 17 applies only to a person that:
- 18 (1) conducts business in this state or produces a
- 19 product or service consumed by residents of this state;
- 20 (2) processes or engages in the sale of personal data;
- 21 <u>and</u>
- 22 (3) is not a small business as defined by the United
- 23 States Small Business Administration, except to the extent that
- 24 Section 541.107 applies to a person described by this subdivision.
- 25 (b) This chapter does not apply to:
- 26 (1) a state agency or a political subdivision of this
- 27 state;

1	(2) a financial institution or data subject to Title
2	V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.);
3	(3) a covered entity or business associate governed by
4	the privacy, security, and breach notification rules issued by the
5	United States Department of Health and Human Services, 45 C.F.R.
6	Parts 160 and 164, established under the Health Insurance
7	Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d
8	et seq.), and the Health Information Technology for Economic and
9	Clinical Health Act (Division A, Title XIII, and Division B, Title
10	IV, Pub. L. No. 111-5);
11	(4) a nonprofit organization; or
12	(5) an institution of higher education.
13	Sec. 541.003. CERTAIN INFORMATION EXEMPT FROM CHAPTER. The
14	following information is exempt from this chapter:
15	(1) protected health information under the Health
16	Insurance Portability and Accountability Act of 1996 (42 U.S.C.
17	Section 1320d et seq.);
18	(2) health records;
19	(3) patient identifying information for purposes of 42
20	U.S.C. Section 290dd-2;
21	(4) identifiable private information:
22	(A) for purposes of the federal policy for the
23	protection of human subjects under 45 C.F.R. Part 46;
24	(B) collected as part of human subjects research
25	under the good clinical practice guidelines issued by The
26	International Council for Harmonisation of Technical Requirements

27 for Pharmaceuticals for Human Use (ICH) or of the protection of

- 1 human subjects under 21 C.F.R. Parts 50 and 56; or
- 2 (C) that is personal data used or shared in
- 3 research conducted in accordance with the requirements set forth in
- 4 this chapter or other research conducted in accordance with
- 5 applicable law;
- 6 (5) information and documents created for purposes of
- 7 the Health Care Quality Improvement Act of 1986 (42 U.S.C. Section
- 8 11101 et seq.);
- 9 (6) patient safety work product for purposes of the
- 10 Patient Safety and Quality Improvement Act of 2005 (42 U.S.C.
- 11 Section 299b-21 et seq.);
- 12 (7) information derived from any of the health
- 13 care-related information listed in this section that is
- 14 deidentified in accordance with the requirements for
- 15 deidentification under the Health Insurance Portability and
- 16 Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.);
- 17 (8) information originating from, and intermingled to
- 18 be indistinguishable with, or information treated in the same
- 19 manner as, information exempt under this section that is maintained
- 20 by a covered entity or business associate as defined by the Health
- 21 Insurance Portability and Accountability Act of 1996 (42 U.S.C.
- 22 Section 1320d et seq.) or by a program or a qualified service
- 23 organization as defined by 42 U.S.C. Section 290dd-2;
- 24 (9) information that is included in a limited data set
- as described by 45 C.F.R. Section 164.514(e), to the extent that the
- 26 information is used, disclosed, and maintained in the manner
- 27 specified by 45 C.F.R. Section 164.514(e);

```
H.B. No. 4
```

- 1 (10) information collected or used only for public
- 2 health activities and purposes as authorized by the Health
- 3 Insurance Portability and Accountability Act of 1996 (42 U.S.C.
- 4 Section 1320d et seq.);
- 5 (11) the collection, maintenance, disclosure, sale,
- 6 communication, or use of any personal information bearing on a
- 7 consumer's creditworthiness, credit standing, credit capacity,
- 8 character, general reputation, personal characteristics, or mode
- 9 of living by a consumer reporting agency or furnisher that provides
- 10 information for use in a consumer report, and by a user of a
- 11 consumer report, but only to the extent that the activity is
- 12 regulated by and authorized under the Fair Credit Reporting Act (15
- 13 U.S.C. Section 1681 et seq.);
- 14 (12) personal data collected, processed, sold, or
- 15 disclosed in compliance with the Driver's Privacy Protection Act of
- 16 <u>1994 (18 U.S.C. Section 2721 et seq.);</u>
- 17 (13) personal data regulated by the Family Educational
- 18 Rights and Privacy Act of 1974 (20 U.S.C. Section 1232g);
- 19 (14) personal data collected, processed, sold, or
- 20 disclosed in compliance with the Farm Credit Act of 1971 (12 U.S.C.
- 21 <u>Section 2001 et seq.);</u>
- 22 (15) data processed or maintained in the course of an
- 23 individual applying to, being employed by, or acting as an agent or
- 24 independent contractor of a controller, processor, or third party,
- 25 to the extent that the data is collected and used within the context
- 26 of that role;
- 27 (16) data processed or maintained as the emergency

- 1 contact information of an individual under this chapter that is
- 2 used for emergency contact purposes; or
- 3 (17) data that is processed or maintained and is
- 4 necessary to retain to administer benefits for another individual
- 5 that relates to an individual described by Subdivision (15) and
- 6 used for the purposes of administering those benefits.
- 7 Sec. 541.004. INAPPLICABILITY OF CHAPTER. This chapter
- 8 does not apply to the processing of personal data by a person in the
- 9 course of a purely personal or household activity.
- 10 Sec. 541.005. EFFECT OF COMPLIANCE WITH PARENTAL CONSENT
- 11 REQUIREMENTS UNDER CERTAIN FEDERAL LAW. A controller or processor
- 12 that complies with the verifiable parental consent requirements of
- 13 the Children's Online Privacy Protection Act (15 U.S.C. Section
- 14 6501 et seq.) with respect to data collected online is considered to
- 15 be in compliance with any requirement to obtain parental consent
- 16 under this chapter.
- SUBCHAPTER B. CONSUMER'S RIGHTS
- 18 Sec. 541.051. CONSUMER'S PERSONAL DATA RIGHTS; REQUEST TO
- 19 EXERCISE RIGHTS. (a) A consumer is entitled to exercise the
- 20 consumer rights authorized by this section at any time by
- 21 submitting a request to a controller specifying the consumer rights
- 22 the consumer wishes to exercise. With respect to the processing of
- 23 personal data belonging to a known child, a parent or legal guardian
- 24 of the child may exercise the consumer rights on behalf of the
- 25 child.
- 26 (b) A controller shall comply with an authenticated
- 27 consumer request to exercise the right to:

1	(1) confirm whether a controller is processing the
2	consumer's personal data and to access the personal data;
3	(2) correct inaccuracies in the consumer's personal
4	data, taking into account the nature of the personal data and the
5	purposes of the processing of the consumer's personal data;
6	(3) delete personal data provided by or obtained about
7	the consumer;
8	(4) if the data is available in a digital format,
9	obtain a copy of the consumer's personal data that the consumer
10	previously provided to the controller in a portable and, to the
11	extent technically feasible, readily usable format that allows the
12	consumer to transmit the data to another controller without
13	hindrance; or
14	(5) opt out of the processing of the personal data for
15	<pre>purposes of:</pre>
16	(A) targeted advertising;
17	(B) the sale of personal data; or
18	(C) profiling in furtherance of a decision that
19	produces a legal or similarly significant effect concerning the
20	<pre>consumer.</pre>
21	Sec. 541.052. CONTROLLER RESPONSE TO CONSUMER REQUEST. (a)
22	Except as otherwise provided by this chapter, a controller shall
23	comply with a request submitted by a consumer to exercise the
24	consumer's rights pursuant to Section 541.051 as provided by this
25	section.
26	(b) A controller shall respond to the consumer request
27	without undue delay, which may not be later than the 45th day after

- 1 the date of receipt of the request. The controller may extend the
- 2 response period once by an additional 45 days when reasonably
- 3 necessary, taking into account the complexity and number of the
- 4 consumer's requests, so long as the controller informs the consumer
- 5 of the extension within the initial 45-day response period,
- 6 together with the reason for the extension.
- 7 (c) If a controller declines to take action regarding the
- 8 consumer's request, the controller shall inform the consumer
- 9 without undue delay, which may not be later than the 45th day after
- 10 the date of receipt of the request, of the justification for
- 11 declining to take action and provide instructions on how to appeal
- 12 the decision in accordance with Section 541.053.
- 13 (d) A controller shall provide information in response to a
- 14 consumer request free of charge, at least twice annually per
- 15 consumer. If a request from a consumer is manifestly unfounded,
- 16 excessive, or repetitive, the controller may charge the consumer a
- 17 reasonable fee to cover the administrative costs of complying with
- 18 the request or may decline to act on the request. The controller
- 19 bears the burden of demonstrating for purposes of this subsection
- 20 that a request is manifestly unfounded, excessive, or repetitive.
- (e) If a controller is unable to authenticate the request
- 22 using commercially reasonable efforts, the controller is not
- 23 required to comply with a consumer request submitted under Section
- 24 541.051 and may request that the consumer provide additional
- 25 information reasonably necessary to authenticate the consumer and
- 26 the consumer's request.
- 27 (f) A controller that has obtained personal data about a

- 1 consumer from a source other than the consumer is considered in
- 2 compliance with a consumer's request to delete that personal data
- 3 pursuant to Section 541.051(b)(3) by:
- 4 (1) retaining a record of the deletion request and the
- 5 minimum data necessary for the purpose of ensuring the consumer's
- 6 personal data remains deleted from the business's records and not
- 7 using the retained data for any other purpose under this chapter; or
- 8 (2) opting the consumer out of the processing of that
- 9 personal data for any purpose other than a purpose that is exempt
- 10 under the provisions of this chapter.
- 11 Sec. 541.053. APPEAL. (a) A controller shall establish a
- 12 process for a consumer to appeal the controller's refusal to take
- 13 action on a request within a reasonable period of time after the
- 14 consumer's receipt of the decision under Section 541.052(c).
- 15 (b) The appeal process must be conspicuously available and
- 16 similar to the process for initiating action to exercise consumer
- 17 rights by submitting a request under Section 541.051.
- 18 (c) A controller shall inform the consumer in writing of any
- 19 action taken or not taken in response to an appeal under this
- 20 section not later than the 60th day after the date of receipt of the
- 21 appeal, including a written explanation of the reason or reasons
- 22 for the decision.
- 23 <u>(d) If the controller denies an appeal, the controller shall</u>
- 24 provide the consumer with the online mechanism described by Section
- 25 541.152 through which the consumer may contact the attorney general
- 26 to submit a complaint.
- Sec. 541.054. WAIVER OR LIMITATION OF CONSUMER RIGHTS

- 1 PROHIBITED. Any provision of a contract or agreement that waives or
- 2 limits in any way a consumer right described by Sections 541.051,
- 3 541.052, and 541.053 is contrary to public policy and is void and
- 4 unenforceable.
- 5 Sec. 541.055. METHODS FOR SUBMITTING CONSUMER REQUESTS.
- 6 (a) A controller shall establish two or more secure and reliable
- 7 methods to enable consumers to submit a request to exercise their
- 8 consumer rights under this chapter. The methods must take into
- 9 account:
- 10 (1) the ways in which consumers normally interact with
- 11 the controller;
- 12 (2) the necessity for secure and reliable
- 13 communications of those requests; and
- 14 (3) the ability of the controller to authenticate the
- 15 identity of the consumer making the request.
- 16 (b) A controller may not require a consumer to create a new
- 17 account to exercise the consumer's rights under this subchapter but
- 18 may require a consumer to use an existing account.
- 19 (c) Except as provided by Subsection (d), if the controller
- 20 maintains an Internet website, the controller must provide a
- 21 mechanism on the website for consumers to submit requests for
- 22 <u>information required to be disclosed under this chapter.</u>
- 23 <u>(d) A controller that operates exclusively online and has a</u>
- 24 direct relationship with a consumer from whom the controller
- 25 collects personal information is only required to provide an e-mail
- 26 address for the submission of requests described by Subsection (c).
- 27 SUBCHAPTER C. CONTROLLER AND PROCESSOR DATA-RELATED DUTIES AND

1	PROHIBITIONS
2	Sec. 541.101. CONTROLLER DUTIES; TRANSPARENCY. (a) A
3	<pre>controller:</pre>
4	(1) shall limit the collection of personal data to
5	what is adequate, relevant, and reasonably necessary in relation to
6	the purposes for which that personal data is processed, as
7	disclosed to the consumer; and
8	(2) for purposes of protecting the confidentiality,
9	integrity, and accessibility of personal data, shall establish,
10	implement, and maintain reasonable administrative, technical, and
11	physical data security practices that are appropriate to the volume
12	and nature of the personal data at issue.
13	(b) A controller may not:
14	(1) except as otherwise provided by this chapter,
15	process personal data for a purpose that is neither reasonably
16	necessary to nor compatible with the disclosed purpose for which
17	the personal data is processed, as disclosed to the consumer,
18	unless the controller obtains the consumer's consent;
19	(2) process personal data in violation of state and
20	federal laws that prohibit unlawful discrimination against
21	<pre>consumers;</pre>
22	(3) discriminate against a consumer for exercising any
23	of the consumer rights contained in this chapter, including by
24	denying goods or services, charging different prices or rates for
25	goods or services, or providing a different level of quality of
26	goods or services to the consumer; or
27	(4) process the sensitive data of a consumer without

- 1 obtaining the consumer's consent, or, in the case of processing the
- 2 sensitive data of a known child, without processing that data in
- 3 accordance with the Children's Online Privacy Protection Act (15
- 4 U.S.C. Section 6501 et seq.).
- 5 (c) Subsection (b)(3) may not be construed to require a
- 6 controller to provide a product or service that requires the
- 7 personal data of a consumer that the controller does not collect or
- 8 maintain or to prohibit a controller from offering a different
- 9 price, rate, level, quality, or selection of goods or services to a
- 10 consumer, including offering goods or services for no fee, if the
- 11 consumer has exercised the consumer's right to opt out under
- 12 Section 541.051 or the offer is related to a consumer's voluntary
- 13 participation in a bona fide loyalty, rewards, premium features,
- 14 discounts, or club card program.
- Sec. 541.102. PRIVACY NOTICE. (a) A controller shall
- 16 provide consumers with a reasonably accessible and clear privacy
- 17 notice that includes:
- 18 (1) the categories of personal data processed by the
- 19 controller, including, if applicable, any sensitive data processed
- 20 by the controller;
- 21 (2) the purpose for processing personal data;
- 22 (3) how consumers may exercise their consumer rights
- 23 under Subchapter B, including the process by which a consumer may
- 24 appeal a controller's decision with regard to the consumer's
- 25 request;
- 26 (4) if applicable, the categories of personal data
- 27 that the controller shares with third parties;

- 1 (5) if applicable, the categories of third parties
- 2 with whom the controller shares personal data; and
- 3 (6) a description of the methods required under
- 4 Section 541.055 through which consumers can submit requests to
- 5 exercise their consumer rights under this chapter.
- 6 (b) If a controller engages in the sale of personal data
- 7 that is sensitive data, the controller shall include the following
- 8 notice:
- 9 "NOTICE: This website may sell your sensitive personal data."
- 10 The notice must be posted in the same location and in the same
- 11 manner as the privacy notice described by Subsection (a).
- 12 (c) If a controller engages in the sale of personal data
- 13 that is biometric data, the controller shall include the following
- 14 notice:
- 15 "NOTICE: This website may sell your biometric personal data."
- 16 The notice must be posted in the same location and in the same
- 17 manner as the privacy notice described by Subsection (a).
- 18 Sec. 541.103. SALE OF DATA TO THIRD PARTIES AND PROCESSING
- 19 DATA FOR TARGETED ADVERTISING; DISCLOSURE. If a controller sells
- 20 personal data to third parties or processes personal data for
- 21 targeted advertising, the controller shall clearly and
- 22 conspicuously disclose that process and the manner in which a
- 23 consumer may exercise the right to opt out of that process.
- Sec. 541.104. DUTIES OF PROCESSOR. (a) A processor shall
- 25 adhere to the instructions of a controller and shall assist the
- 26 controller in meeting or complying with the controller's duties or
- 27 requirements under this chapter, including:

1	(1) assisting the controller in responding to consumer
2	rights requests submitted under Section 541.051 by using
3	appropriate technical and organizational measures, as reasonably
4	practicable, taking into account the nature of processing and the
5	information available to the processor;
6	(2) assisting the controller with regard to complying
7	with the requirement relating to the security of processing
8	personal data and to the notification of a breach of security of the
9	processor's system under Chapter 521, taking into account the
10	nature of processing and the information available to the
11	processor; and
12	(3) providing necessary information to enable the
13	controller to conduct and document data protection assessments
14	under Section 541.105.
15	(b) A contract between a controller and a processor shall
16	govern the processor's data processing procedures with respect to
17	processing performed on behalf of the controller. The contract must
18	<pre>include:</pre>
19	(1) clear instructions for processing data;
20	(2) the nature and purpose of processing;
21	(3) the type of data subject to processing;
22	(4) the duration of processing;
23	(5) the rights and obligations of both parties; and
24	(6) a requirement that the processor shall:
25	(A) ensure that each person processing personal
26	data is subject to a duty of confidentiality with respect to the
27	<pre>data;</pre>

- 1 (B) at the controller's direction, delete or
- 2 return all personal data to the controller as requested after the
- 3 provision of the service is completed, unless retention of the
- 4 personal data is required by law;
- 5 (C) make available to the controller, on
- 6 reasonable request, all information in the processor's possession
- 7 necessary to demonstrate the processor's compliance with the
- 8 requirements of this chapter;
- 9 (D) allow, and cooperate with, reasonable
- 10 assessments by the controller or the controller's designated
- 11 assessor; and
- 12 <u>(E) engage any subcontractor pursuant to a</u>
- 13 written contract that requires the subcontractor to meet the
- 14 requirements of the processor with respect to the personal data.
- 15 <u>(c) Notwithstanding the requirement described by Subsection</u>
- 16 (b)(6)(D), a processor, in the alternative, may arrange for a
- 17 qualified and independent assessor to conduct an assessment of the
- 18 processor's policies and technical and organizational measures in
- 19 support of the requirements under this chapter using an appropriate
- 20 and accepted control standard or framework and assessment
- 21 procedure. The processor shall provide a report of the assessment
- 22 to the controller on request.
- 23 <u>(d) This section may not be construed to relieve a</u>
- 24 controller or a processor from the liabilities imposed on the
- 25 controller or processor by virtue of its role in the processing
- 26 relationship as described by this chapter.
- (e) A determination of whether a person is acting as a

- 1 controller or processor with respect to a specific processing of
- 2 data is a fact-based determination that depends on the context in
- 3 which personal data is to be processed. A processor that continues
- 4 to adhere to a controller's instructions with respect to a specific
- 5 processing of personal data remains in the role of a processor.
- 6 Sec. 541.105. DATA PROTECTION ASSESSMENTS. (a) A
- 7 controller shall conduct and document a data protection assessment
- 8 of each of the following processing activities involving personal
- 9 data:
- 10 <u>(1) the processing of personal data for purposes of</u>
- 11 targeted advertising;
- 12 (2) the sale of personal data;
- 13 (3) the processing of personal data for purposes of
- 14 profiling, if the profiling presents a reasonably foreseeable risk
- 15 <u>of:</u>
- 16 (A) unfair or deceptive treatment of or unlawful
- 17 disparate impact on consumers;
- 18 (B) financial, physical, or reputational injury
- 19 to consumers;
- 20 (C) a physical or other intrusion on the solitude
- 21 or seclusion, or the private affairs or concerns, of consumers, if
- 22 the intrusion would be offensive to a reasonable person; or
- 23 (D) other substantial injury to consumers;
- 24 (4) the processing of sensitive data; and
- 25 (5) any processing activities involving personal data
- 26 that present a heightened risk of harm to consumers.
- 27 (b) A data protection assessment conducted under Subsection

- H.B. No. 4 1 (<u>a) must:</u> 2 (1) identify and weigh the direct or indirect benefits 3 that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against the potential risks to 4 5 the rights of the consumer associated with that processing, as 6 mitigated by safeguards that can be employed by the controller to 7 reduce the risks; and 8 (2) factor into the assessment: 9 (A) the use of deidentified data; 10 (B) the reasonable expectations of consumers; 11 (C) the context of the processing; and 12 (D) the relationship between the controller and 13 the consumer whose personal data will be processed. 14 (c) A controller shall make a data protection assessment requested under Section 541.153(b) available to the attorney
- 15 general pursuant to a civil investigative demand under Section 16 541.153. 17
- 18 (d) A data protection assessment is confidential and exempt 19 from public inspection and copying under Chapter 552, Government 20 Code. Disclosure of a data protection assessment in compliance with 21 a request from the attorney general does not constitute a waiver of 22 attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment. 23
- 24 (e) A single data protection assessment may address a 25 comparable set of processing operations that include similar 26 activities.
- 27 (f) A data protection assessment conducted by a controller

- 1 for the purpose of compliance with other laws or regulations may
- 2 constitute compliance with the requirements of this section if the
- 3 assessment has a reasonably comparable scope and effect.
- 4 Sec. 541.106. DEIDENTIFIED OR PSEUDONYMOUS DATA. (a) A
- 5 controller in possession of deidentified data shall:
- 6 (1) take reasonable measures to ensure that the data
- 7 cannot be associated with an individual;
- 8 (2) publicly commit to maintaining and using
- 9 deidentified data without attempting to reidentify the data; and
- 10 (3) contractually obligate any recipient of the
- 11 deidentified data to comply with the provisions of this chapter.
- 12 (b) This chapter may not be construed to require a
- 13 controller or processor to:
- 14 (1) reidentify deidentified data or pseudonymous
- 15 <u>data;</u>
- 16 (2) maintain data in identifiable form or obtain,
- 17 retain, or access any data or technology for the purpose of allowing
- 18 the controller or processor to associate a consumer request with
- 19 personal data; or
- 20 (3) comply with an authenticated consumer rights
- 21 request under Section 541.051, if the controller:
- (A) is not reasonably capable of associating the
- 23 request with the personal data or it would be unreasonably
- 24 burdensome for the controller to associate the request with the
- 25 personal data;
- 26 (B) does not use the personal data to recognize
- 27 or respond to the specific consumer who is the subject of the

- 1 personal data or associate the personal data with other personal
- 2 data about the same specific consumer; and
- 3 (C) does not sell the personal data to any third
- 4 party or otherwise voluntarily disclose the personal data to any
- 5 third party other than a processor, except as otherwise permitted
- 6 by this section.
- 7 (c) The consumer rights under Sections 541.051(b)(1)-(4)
- 8 and controller duties under Section 541.101 do not apply to
- 9 pseudonymous data in cases in which the controller is able to
- 10 demonstrate any information necessary to identify the consumer is
- 11 kept separately and is subject to effective technical and
- 12 organizational controls that prevent the controller from accessing
- 13 the information.
- 14 (d) A controller that discloses pseudonymous data or
- 15 <u>deidentified data shall exercise reasonable oversight to monitor</u>
- 16 compliance with any contractual commitments to which the
- 17 pseudonymous data or deidentified data is subject and shall take
- 18 appropriate steps to address any breach of the contractual
- 19 commitments.
- Sec. 541.107. REQUIREMENTS FOR SMALL BUSINESSES. (a) A
- 21 person described by Section 541.002(a)(3) may not engage in the
- 22 sale of personal data that is sensitive data without receiving
- 23 prior consent from the consumer.
- 24 (b) A person who violates this section is subject to the
- 25 penalty under Section 541.155.
- SUBCHAPTER D. ENFORCEMENT
- Sec. 541.151. ENFORCEMENT AUTHORITY EXCLUSIVE. The

- 1 attorney general has exclusive authority to enforce this chapter.
- 2 Sec. 541.152. INTERNET WEBSITE AND COMPLAINT MECHANISM.
- 3 The attorney general shall post on the attorney general's Internet
- 4 website:
- 5 (1) information relating to:
- 6 (A) the responsibilities of a controller under
- 7 Subchapters B and C;
- 8 (B) the responsibilities of a processor under
- 9 <u>Subchapter C;</u> and
- 10 (C) a consumer's rights under Subchapter B; and
- 11 (2) an online mechanism through which a consumer may
- 12 submit a complaint under this chapter to the attorney general.
- 13 Sec. 541.153. INVESTIGATIVE AUTHORITY. (a) If the
- 14 attorney general has reasonable cause to believe that a person has
- 15 engaged in, is engaging in, or is about to engage in a violation of
- 16 this chapter, the attorney general may issue a civil investigative
- 17 demand. The procedures established for the issuance of a civil
- 18 investigative demand under Section 15.10 apply to the same extent
- 19 and manner to the issuance of a civil investigative demand under
- 20 this section.
- 21 (b) The attorney general may request, pursuant to a civil
- 22 <u>investigative demand issued under Subsection (a)</u>, that a controller
- 23 disclose any data protection assessment that is relevant to an
- 24 investigation conducted by the attorney general. The attorney
- 25 general may evaluate the data protection assessment for compliance
- 26 with the requirements set forth in Sections 541.101, 541.102, and
- 27 541.103.

H.B. No. 4 1 Sec. 541.154. NOTICE OF VIOLATION OF CHAPTER; OPPORTUNITY 2 TO CURE. Before bringing an action under Section 541.155, the 3 attorney general shall notify a person in writing, not later than the 30th day before bringing the action, identifying the specific 4 5 provisions of this chapter the attorney general alleges have been or are being violated. The attorney general may not bring an action 6 7 against the person if: 8 (1) within the 30-day period, the person cures the identified violation; and 9 10 (2) the person provides the attorney general a written statement that the person: 11 12 (A) cured the alleged violation; (B) notified the consumer that the consumer's 13 privacy violation was addressed; 14 15 (C) provided supportive documentation to show 16 how the privacy violation was cured; and 17 (D) made changes to internal policies to ensure 18 that no further violations will occur. 19 Sec. 541.155. CIVIL PENALTY; INJUNCTION. (a) A person who violates this chapter following the cure period described by 20 Section 541.154 or who breaches a written statement provided to the 21 22 attorney general under that section is liable for a civil penalty in an amount not to exceed \$7,500 for each violation. 23

(1) recover a civil penalty under this section;

The attorney general may bring an action in the name of

(2) restrain or enjoin the person from violating this

24

25

26

27

(b)

this state to:

- 1 chapter; or
- 2 (3) recover the civil penalty and seek injunctive
- 3 relief.
- 4 (c) The attorney general may recover reasonable attorney's
- 5 fees and other reasonable expenses incurred in investigating and
- 6 bringing an action under this section.
- 7 (d) The attorney general shall deposit a civil penalty
- 8 collected under this section in the state treasury to the credit of
- 9 the general revenue fund.
- Sec. 541.156. NO PRIVATE RIGHT OF ACTION. This chapter may
- 11 not be construed as providing a basis for, or being subject to, a
- 12 private right of action for a violation of this chapter or any other
- 13 law.
- 14 SUBCHAPTER E. CONSTRUCTION OF CHAPTER; EXEMPTIONS FOR CERTAIN USES
- OF CONSUMER PERSONAL DATA
- Sec. 541.201. CONSTRUCTION OF CHAPTER. (a) This chapter
- 17 may not be construed to restrict a controller's or processor's
- 18 ability to:
- 19 (1) comply with federal, state, or local laws, rules,
- 20 or regulations;
- 21 (2) comply with a civil, criminal, or regulatory
- 22 inquiry, investigation, subpoena, or summons by federal, state,
- 23 <u>local</u>, or other governmental authorities;
- 24 (3) investigate, establish, exercise, prepare for, or
- 25 defend legal claims;
- 26 (4) provide a product or service specifically
- 27 requested by a consumer or the parent or guardian of a child,

- 1 perform a contract to which the consumer is a party, including
- 2 fulfilling the terms of a written warranty, or take steps at the
- 3 request of the consumer before entering into a contract;
- 4 (5) take immediate steps to protect an interest that
- 5 is essential for the life or physical safety of the consumer or of
- 6 another individual and in which the processing cannot be manifestly
- 7 <u>based on another legal basis;</u>
- 8 (6) prevent, detect, protect against, or respond to
- 9 security incidents, identity theft, fraud, harassment, malicious
- 10 or deceptive activities, or any illegal activity;
- 11 (7) preserve the integrity or security of systems or
- 12 investigate, report, or prosecute those responsible for breaches of
- 13 system security;
- 14 (8) engage in public or peer-reviewed scientific or
- 15 statistical research in the public interest that adheres to all
- 16 other applicable ethics and privacy laws and is approved,
- 17 monitored, and governed by an institutional review board or similar
- 18 independent oversight entity that determines:
- 19 (A) if the deletion of the information is likely
- 20 to provide substantial benefits that do not exclusively accrue to
- 21 the controller;
- (B) whether the expected benefits of the research
- 23 <u>outweigh the privacy risks; and</u>
- (C) if the controller has implemented reasonable
- 25 safeguards to mitigate privacy risks associated with research,
- 26 including any risks associated with reidentification; or
- 27 (9) assist another controller, processor, or third

- 1 party with any of the requirements under this subsection.
- 2 (b) This chapter may not be construed to prevent a
- 3 controller or processor from providing personal data concerning a
- 4 consumer to a person covered by an evidentiary privilege under the
- 5 laws of this state as part of a privileged communication.
- 6 (c) This chapter may not be construed as imposing a
- 7 requirement on controllers and processors that adversely affects
- 8 the rights or freedoms of any person, including the right of free
- 9 speech.
- 10 (d) This chapter may not be construed as requiring a
- 11 controller, processor, third party, or consumer to disclose a trade
- 12 secret.
- 13 Sec. 541.202. COLLECTION, USE, OR RETENTION OF DATA FOR
- 14 CERTAIN PURPOSES. (a) The requirements imposed on controllers and
- 15 processors under this chapter may not restrict a controller's or
- 16 processor's ability to collect, use, or retain data to:
- 17 (1) conduct internal research to develop, improve, or
- 18 repair products, services, or technology;
- 19 (2) effect a product recall;
- 20 (3) identify and repair technical errors that impair
- 21 <u>existing or intended functionality; or</u>
- 22 (4) perform internal operations that:
- 23 (A) are reasonably aligned with the expectations
- 24 of the consumer;
- (B) are reasonably anticipated based on the
- 26 consumer's existing relationship with the controller; or
- (C) are otherwise compatible with processing

- 1 data in furtherance of the provision of a product or service
- 2 specifically requested by a consumer or the performance of a
- 3 contract to which the consumer is a party.
- 4 (b) A requirement imposed on a controller or processor under
- 5 this chapter does not apply if compliance with the requirement by
- 6 the controller or processor, as applicable, would violate an
- 7 evidentiary privilege under the laws of this state.
- 8 Sec. 541.203. DISCLOSURE OF PERSONAL DATA TO THIRD-PARTY
- 9 CONTROLLER OR PROCESSOR. (a) A controller or processor that
- 10 discloses personal data to a third-party controller or processor,
- 11 in compliance with the requirements of this chapter, does not
- 12 violate this chapter if the third-party controller or processor
- 13 that receives and processes that personal data is in violation of
- 14 this chapter, provided that, at the time of the data's disclosure,
- 15 the disclosing controller or processor did not have actual
- 16 knowledge that the recipient intended to commit a violation.
- 17 (b) A third-party controller or processor receiving
- 18 personal data from a controller or processor in compliance with the
- 19 requirements of this chapter does not violate this chapter for the
- 20 transgressions of the controller or processor from which the
- 21 third-party controller or processor receives the personal data.
- Sec. 541.204. PROCESSING OF CERTAIN PERSONAL DATA BY
- 23 CONTROLLER OR OTHER PERSON. (a) Personal data processed by a
- 24 controller under this subchapter may not be processed for any
- 25 purpose other than a purpose listed in this subchapter unless
- 26 otherwise allowed by this chapter. Personal data processed by a
- 27 controller under this subchapter may be processed to the extent

- 1 that the processing of the data is:
- 2 (1) reasonably necessary and proportionate to the
- 3 purposes listed in this subchapter; and
- 4 (2) adequate, relevant, and limited to what is
- 5 necessary in relation to the specific purposes listed in this
- 6 subchapter.
- 7 (b) Personal data collected, used, or retained under
- 8 Section 541.202(a) must, where applicable, take into account the
- 9 nature and purpose of such collection, use, or retention. The
- 10 personal data described by this subsection is subject to reasonable
- 11 administrative, technical, and physical measures to protect the
- 12 confidentiality, integrity, and accessibility of the personal data
- 13 and to reduce reasonably foreseeable risks of harm to consumers
- 14 relating to the collection, use, or retention of personal data.
- 15 <u>(c) A controller that processes personal data under an</u>
- 16 <u>exemption in this subchapter bears the burden of demonstrating that</u>
- 17 the processing of the personal data qualifies for the exemption and
- 18 complies with the requirements of Subsections (a) and (b).
- 19 <u>(d) The processing of personal data by an entity for the</u>
- 20 purposes described by Section 541.201 does not solely make the
- 21 entity a controller with respect to the processing of the data.
- 22 <u>Sec. 541.205. LOCAL PREEMPTION. This chapter supersedes</u>
- 23 and preempts any ordinance, resolution, rule, or other regulation
- 24 adopted by a political subdivision regarding the processing of
- 25 personal data by a controller or processor.
- 26 SECTION 3. (a) The Department of Information Resources,
- 27 under the management of the chief privacy officer, shall review the

H.B. No. 4

- 1 implementation of the requirements of Chapter 541, Business &
- 2 Commerce Code, as added by this Act.
- 3 (b) Not later than September 1, 2024, the Department of
- 4 Information Resources shall create an online portal available on
- 5 the department's Internet website for members of the public to
- 6 provide feedback and recommend changes to Chapter 541, Business &
- 7 Commerce Code, as added by this Act. The online portal must remain
- 8 open for receiving feedback from the public for at least 90 days.
- 9 (c) Not later than January 1, 2025, the Department of
- 10 Information Resources shall make available to the public a report
- 11 detailing the status of the implementation of the requirements of
- 12 Chapter 541, Business & Commerce Code, as added by this Act, and any
- 13 recommendations to the legislature regarding changes to that law.
- 14 (d) This section expires September 1, 2025.
- 15 SECTION 4. Data protection assessments required to be
- 16 conducted under Section 541.105, Business & Commerce Code, as added
- 17 by this Act, apply only to processing activities generated after
- 18 the effective date of this Act and are not retroactive.
- 19 SECTION 5. Not later than March 1, 2024, the attorney
- 20 general shall post the information and online mechanism required by
- 21 Section 541.152, Business & Commerce Code, as added by this Act.
- 22 SECTION 6. The provisions of this Act are hereby declared
- 23 severable, and if any provision of this Act or the application of
- 24 such provision to any person or circumstance is declared invalid
- 25 for any reason, such declaration shall not affect the validity of
- 26 the remaining portions of this Act.
- 27 SECTION 7. This Act takes effect March 1, 2024.

ADOPTED

MAY 10 2023

By: Super Langles

H.B. No. 4

Substitute the following for H.B. No. H:

B/ Super profee

c.s.<u>H</u>.B. No. <u>4</u>

## A BILL TO BE ENTITLED

1 AN ACT relating to the regulation of the collection, use, processing, and 2 treatment of consumers' personal data by certain business entities; 3 imposing a civil penalty. 4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS: 5 SECTION 1. This Act may be cited as the Texas Data Privacy 6 7 and Security Act. 8 SECTION 2. Title 11, Business & Commerce Code, is amended by adding Subtitle C to read as follows: 9 SUBTITLE C. CONSUMER DATA PROTECTION 10 CHAPTER 541. CONSUMER DATA PROTECTION 11 SUBCHAPTER A. GENERAL PROVISIONS 12 13 Sec. 541.001. DEFINITIONS. In this chapter, unless a different meaning is required by the context: 14 (1) "Affiliate" means a legal entity that controls, is 15 controlled by, or is under common control with another legal entity 16 or shares common branding with another legal entity. For purposes 17 of this subdivision, "control" or "controlled" means: 18 (A) the ownership of, or power to vote, more than 19 50 percent of the outstanding shares of any class of voting security 20 21 of a company; (B) the control in any manner over the election 22 of a majority of the directors or of individuals exercising similar 23

functions; or

24

- 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 <u>of age.</u>
- (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 <u>include:</u>
- 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 <u>impairing user autonomy, decision-making, or choice, and includes</u>
- 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	<pre>controller of:</pre>
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;
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; or
25	(E) a subsidiary or affiliate of an entity
26	regulated under Subtitle B, Title 2, Utilities Code.
27	(19) "Personal data" means any information, including

```
1
   sensitive data, that is linked or reasonably linkable to an
   identified or identifiable individual. The term includes
2
3
   pseudonymous data when the data is used by a controller or processor
   in conjunction with additional information that reasonably links
4
5
   the data to an identified or identifiable individual. The term does
   not include deidentified data or publicly available information.
6
7
               (20) "Political organization" means a party,
   committee, association, fund, or other organization, regardless of
8
   whether incorporated, that is organized and operated primarily for
9
10
   the purpose of influencing or attempting to influence:
                    (A) the selection, nomination, election, or
11
12
   appointment of an individual to a federal, state, or local public
   office or an office in a political organization, regardless of
13
   whether the individual is selected, nominated, elected, or
14
15
   appointed; or
16
                    (B) the
                                     election
                                                      of
17
   presidential/vice-presidential elector, regardless of whether the
18
   elector is selected, nominated, elected, or appointed.
               (21) "Precise geolocation data" means information
19
20
   derived from technology, including global positioning system level
   latitude and longitude coordinates or other mechanisms, that
21
22
   directly identifies the specific location of an individual with
```

or to equipment for use by a utility.

23

24

25

26

27

precision and accuracy within a radius of 1,750 feet. The term does

not include the content of communications or any data generated by

or connected to an advanced utility metering infrastructure system

(22) "Process" or "processing" means an operation or

- 1 set of operations performed, whether by manual or automated means,
- 2 on personal data or on sets of personal data, such as the
- 3 collection, use, storage, disclosure, analysis, deletion, or
- 4 modification of personal data.
- 5 (23) "Processor" means a person that processes
- 6 personal data on behalf of a controller.
- 7 (24) "Profiling" means any form of solely automated
- 8 processing performed on personal data to evaluate, analyze, or
- 9 predict personal aspects related to an identified or identifiable
- 10 individual's economic situation, health, personal preferences,
- 11 <u>interests</u>, reliability, behavior, location, or movements.
- 12 (25) "Protected health information" has the meaning
- 13 assigned to the term by the Health Insurance Portability and
- 14 Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).
- 15 (26) "Pseudonymous data" means any information that
- 16 cannot be attributed to a specific individual without the use of
- 17 additional information, provided that the additional information
- 18 is kept separately and is subject to appropriate technical and
- 19 organizational measures to ensure that the personal data is not
- 20 attributed to an identified or identifiable individual.
- 21 (27) "Publicly available information" means
- 22 <u>information that is lawfully made available through government</u>
- 23 records, or information that a business has a reasonable basis to
- 24 believe is lawfully made available to the general public through
- 25 widely distributed media, by a consumer, or by a person to whom a
- 26 consumer has disclosed the information, unless the consumer has
- 27 <u>restricted the information to a specific audience.</u>

```
1
               (28) "Sale of personal data" means the sharing,
 2
   disclosing, or transferring of personal data for monetary or other
   valuable consideration by the controller to a third party. The term
 3
   does not include:
 4
 5
                    (A) the disclosure of personal data to a
 6
   processor that processes the personal data on the controller's
 7
   behalf;
8
                    (B) the disclosure of personal data to a third
9
   party for purposes of providing a product or service requested by
10
   the consumer;
11
                    (C) the disclosure or transfer of personal data
   to an affiliate of the controller;
12
13
                    (D) the disclosure of information that the
14
   consumer:
                         (i) intentionally made available to the
15
   general public through a mass media channel; and
16
17
                         (ii) did not restrict to a specific
18
   audience; or
19
                    (E) the disclosure or transfer of personal data
   to a third party as an asset that is part of a merger or acquisition.
20
21
               (29) "Sensitive data" means a category of personal
22
   data. The term includes:
23
                    (A) personal data revealing racial or ethnic
24
   origin, religious beliefs, mental or physical health diagnosis, or
25
   citizenship or immigration status;
26
                    (B) genetic or biometric data that is processed
```

for the purpose of uniquely identifying an individual;

```
1
                    (C) personal data collected from a known child;
2
   or
3
                    (D) precise geolocation data.
4
               (30) "State agency" means a department, commission,
   board, office, council, authority, or other agency in the executive
5
   branch of state government that is created by the constitution or a
6
7
   statute of this state, including a university system or institution
8
   of higher education as defined by Section 61.003, Education Code.
               (31) "Targeted advertising" means displaying to a
9
   consumer an advertisement that is selected based on personal data
10
   obtained from that consumer's activities over time and across
11
12
   nonaffiliated websites or online applications to predict the
   consumer's preferences or interests. The term does not include:
13
14
                    (A) an advertisement that:
15
                         (i) is based on activities within a
16
   controller's own websites or online applications;
17
                         (ii) is based on the context of a consumer's
18
   current search query, visit to a website, or online application; or
19
                         (iii) is directed to a consumer in response
   to the consumer's request for information or feedback; or
20
21
                    (B) the processing of personal data solely for
   measuring or reporting advertising performance, reach, or
22
23
   frequency.
24
               (32) "Third party" means a person, other than the
   consumer, the controller, the processor, or an affiliate of the
25
   controller or processor.
26
               (33) "Trade secret" means all forms and types of
27
```

- 1 information, including business, scientific, technical, economic,
- 2 or engineering information, and any formula, design, prototype,
- 3 pattern, plan, compilation, program device, program, code, device,
- 4 method, technique, process, procedure, financial data, or list of
- 5 actual or potential customers or suppliers, whether tangible or
- 6 intangible and whether or how stored, compiled, or memorialized
- 7 physically, electronically, graphically, photographically, or in
- 8 writing if:
- 9 (A) the owner of the trade secret has taken
- 10 reasonable measures under the circumstances to keep the information
- 11 secret; and
- 12 (B) the information derives independent economic
- 13 value, actual or potential, from not being generally known to, and
- 14 not being readily ascertainable through proper means by, another
- 15 person who can obtain economic value from the disclosure or use of
- 16 the information.
- Sec. 541.002. APPLICABILITY OF CHAPTER. (a) This chapter
- 18 applies only to a person that:
- 19 (1) conducts business in this state or produces a
- 20 product or service consumed by residents of this state;
- (2) processes or engages in the sale of personal data;
- 22 and
- 23 (3) is not a small business as defined by the United
- 24 States Small Business Administration, except to the extent that
- 25 Section 541.107 applies to a person described by this subdivision.
- (b) This chapter does not apply to:
- 27 (1) a state agency or a political subdivision of this

```
1
    state;
 2
               (2) a financial institution or data subject to Title
 3
    V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.);
 4
               (3) a covered entity or business associate governed by
 5
    the privacy, security, and breach notification rules issued by the
    United States Department of Health and Human Services, 45 C.F.R.
 6
 7
    Parts 160 and 164, established under the Health Insurance
 8
    Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d
 9
    et seq.), and the Health Information Technology for Economic and
    Clinical Health Act (Division A, Title XIII, and Division B, Title
10
11
    IV, Pub. L. No. 111-5);
12
               (4) a nonprofit organization;
13
               (5) an institution of higher education; or
14
               (6) an electric utility, a power generation company,
    or a retail electric provider, as those terms are defined by Section
15
16
    31.002, Utilities Code.
          Sec. 541.003. CERTAIN INFORMATION EXEMPT FROM CHAPTER.
17
18
    following information is exempt from this chapter:
19
               (1) protected health information under the Health
20
    Insurance Portability and Accountability Act of 1996 (42 U.S.C.
21
   Section 1320d et seq.);
22
               (2) health records;
23
               (3) patient identifying information for purposes of 42
24
   U.S.C. Section 290dd-2;
25
               (4) identifiable private information:
26
                    (A) for purposes of the federal policy for the
27
   protection of human subjects under 45 C.F.R. Part 46;
```

```
1
                    (B) collected as part of human subjects research
 2
   under the good clinical practice guidelines issued by The
   International Council for Harmonisation of Technical Requirements
 3
   for Pharmaceuticals for Human Use (ICH) or of the protection of
 4
   human subjects under 21 C.F.R. Parts 50 and 56; or
 5
 6
                    (C) that is personal data used or shared in
 7
   research conducted in accordance with the requirements set forth in
 8
   this chapter or other research conducted in accordance with
 9
   applicable law;
10
               (5) information and documents created for purposes of
   the Health Care Quality Improvement Act of 1986 (42 U.S.C. Section
11
12
   11101 et seq.);
13
               (6) patient safety work product for purposes of the
14
   Patient Safety and Quality Improvement Act of 2005 (42 U.S.C.
   Section 299b-21 et seq.);
15
16
               (7) information derived from any of the health
   care-related information listed in this section that
17
                                                                is
18
   deidentified in accordance with
                                          the requirements
                                                                for
   deidentification under the Health Insurance Portability and
19
20
   Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.);
21
              (8) information originating from, and intermingled to
22
   be indistinguishable with, or information treated in the same
23
   manner as, information exempt under this section that is maintained
24
   by a covered entity or business associate as defined by the Health
25
   Insurance Portability and Accountability Act of 1996 (42 U.S.C.
26
   Section 1320d et seq.) or by a program or a qualified service
```

organization as defined by 42 U.S.C. Section 290dd-2;

```
1
               (9) information that is included in a limited data set
 2
   as described by 45 C.F.R. Section 164.514(e), to the extent that the
   information is used, disclosed, and maintained in the manner
 3
   specified by 45 C.F.R. Section 164.514(e);
 4
5
               (10) information collected or used only for public
   health activities and purposes as authorized by the Health
6
7
   Insurance Portability and Accountability Act of 1996 (42 U.S.C.
8
   Section 1320d et seq.);
9
               (11) the collection, maintenance, disclosure, sale,
   communication, or use of any personal information bearing on a
10
11
   consumer's creditworthiness, credit standing, credit capacity,
12
   character, general reputation, personal characteristics, or mode
13
   of living by a consumer reporting agency or furnisher that provides
14
   information for use in a consumer report, and by a user of a
   consumer report, but only to the extent that the activity is
15
16
   regulated by and authorized under the Fair Credit Reporting Act (15
17
   U.S.C. Section 1681 et seq.);
               (12) personal data collected, processed, sold, or
18
19
   disclosed in compliance with the Driver's Privacy Protection Act of
20
   1994 (18 U.S.C. Section 2721 et seq.);
21
               (13) personal data regulated by the Family Educational
22
   Rights and Privacy Act of 1974 (20 U.S.C. Section 1232g);
23
               (14) personal data collected, processed, sold, or
```

Section 2001 et seq.);

24

25

26

27

individual applying to, being employed by, or acting as an agent or

disclosed in compliance with the Farm Credit Act of 1971 (12 U.S.C.

(15) data processed or maintained in the course of an

- 1 independent contractor of a controller, processor, or third party,
- 2 to the extent that the data is collected and used within the context
- 3 of that role;
- 4 (16) data processed or maintained as the emergency
- 5 contact information of an individual under this chapter that is
- 6 used for emergency contact purposes; or
- 7 (17) data that is processed or maintained and is
- 8 necessary to retain to administer benefits for another individual
- 9 that relates to an individual described by Subdivision (15) and
- 10 used for the purposes of administering those benefits.
- 11 Sec. 541.004. INAPPLICABILITY OF CHAPTER. This chapter
- 12 does not apply to the processing of personal data by a person in the
- 13 course of a purely personal or household activity.
- 14 Sec. 541.005. EFFECT OF COMPLIANCE WITH PARENTAL CONSENT
- 15 REQUIREMENTS UNDER CERTAIN FEDERAL LAW. A controller or processor
- 16 that complies with the verifiable parental consent requirements of
- 17 the Children's Online Privacy Protection Act of 1998 (15 U.S.C.
- 18 Section 6501 et seq.) with respect to data collected online is
- 19 considered to be in compliance with any requirement to obtain
- 20 parental consent under this chapter.
- SUBCHAPTER B. CONSUMER'S RIGHTS
- Sec. 541.051. CONSUMER'S PERSONAL DATA RIGHTS; REQUEST TO
- 23 EXERCISE RIGHTS. (a) A consumer is entitled to exercise the
- 24 consumer rights authorized by this section at any time by
- 25 submitting a request to a controller specifying the consumer rights
- 26 the consumer wishes to exercise. With respect to the processing of
- 27 personal data belonging to a known child, a parent or legal guardian

- 1 of the child may exercise the consumer rights on behalf of the
- 2 child.
- 3 (b) A controller shall comply with an authenticated
- 4 consumer request to exercise the right to:
- 5 (1) confirm whether a controller is processing the
- 6 consumer's personal data and to access the personal data;
- 7 (2) correct inaccuracies in the consumer's personal
- 8 data, taking into account the nature of the personal data and the
- 9 purposes of the processing of the consumer's personal data;
- 10 (3) delete personal data provided by or obtained about
- 11 the consumer;
- 12 (4) if the data is available in a digital format,
- 13 obtain a copy of the consumer's personal data that the consumer
- 14 previously provided to the controller in a portable and, to the
- 15 extent technically feasible, readily usable format that allows the
- 16 consumer to transmit the data to another controller without
- 17 hindrance; or
- (5) opt out of the processing of the personal data for
- 19 purposes of:
- 20 (A) targeted advertising;
- 21 (B) the sale of personal data; or
- (C) profiling in furtherance of a decision that
- 23 produces a legal or similarly significant effect concerning the
- 24 consumer.
- Sec. 541.052. CONTROLLER RESPONSE TO CONSUMER REQUEST. (a)
- 26 Except as otherwise provided by this chapter, a controller shall
- 27 comply with a request submitted by a consumer to exercise the

- 1 consumer's rights pursuant to Section 541.051 as provided by this
- 2 section.
- 3 (b) A controller shall respond to the consumer request
- 4 without undue delay, which may not be later than the 45th day after
- 5 the date of receipt of the request. The controller may extend the
- 6 response period once by an additional 45 days when reasonably
- 7 necessary, taking into account the complexity and number of the
- 8 consumer's requests, so long as the controller informs the consumer
- 9 of the extension within the initial 45-day response period,
- 10 together with the reason for the extension.
- (c) If a controller declines to take action regarding the
- 12 consumer's request, the controller shall inform the consumer
- 13 without undue delay, which may not be later than the 45th day after
- 14 the date of receipt of the request, of the justification for
- 15 declining to take action and provide instructions on how to appeal
- 16 the decision in accordance with Section 541.053.
- 17 (d) A controller shall provide information in response to a
- 18 consumer request free of charge, at least twice annually per
- 19 consumer. If a request from a consumer is manifestly unfounded,
- 20 excessive, or repetitive, the controller may charge the consumer a
- 21 reasonable fee to cover the administrative costs of complying with
- 22 the request or may decline to act on the request. The controller
- 23 bears the burden of demonstrating for purposes of this subsection
- 24 that a request is manifestly unfounded, excessive, or repetitive.
- 25 (e) If a controller is unable to authenticate the request
- 26 using commercially reasonable efforts, the controller is not
- 27 required to comply with a consumer request submitted under Section

- 1 <u>541.051</u> and may request that the consumer provide additional
- 2 information reasonably necessary to authenticate the consumer and
- 3 the consumer's request.
- 4 (f) A controller that has obtained personal data about a
- 5 consumer from a source other than the consumer is considered in
- 6 compliance with a consumer's request to delete that personal data
- 7 pursuant to Section 541.051(b)(3) by:
- 8 (1) retaining a record of the deletion request and the
- 9 minimum data necessary for the purpose of ensuring the consumer's
- 10 personal data remains deleted from the business's records and not
- 11 using the retained data for any other purpose under this chapter; or
- (2) opting the consumer out of the processing of that
- 13 personal data for any purpose other than a purpose that is exempt
- 14 under the provisions of this chapter.
- Sec. 541.053. APPEAL. (a) A controller shall establish a
- 16 process for a consumer to appeal the controller's refusal to take
- 17 <u>action on a request within a reasonable period of time after the</u>
- 18 consumer's receipt of the decision under Section 541.052(c).
- 19 (b) The appeal process must be conspicuously available and
- 20 similar to the process for initiating action to exercise consumer
- 21 rights by submitting a request under Section 541.051.
- (c) A controller shall inform the consumer in writing of any
- 23 action taken or not taken in response to an appeal under this
- 24 section not later than the 60th day after the date of receipt of the
- 25 appeal, including a written explanation of the reason or reasons
- 26 for the decision.
- 27 <u>(d) If the controller denies an appeal, the controller shall</u>

- 1 provide the consumer with the online mechanism described by Section
- 2 541.152 through which the consumer may contact the attorney general
- 3 to submit a complaint.
- 4 Sec. 541.054. WAIVER OR LIMITATION OF CONSUMER RIGHTS
- 5 PROHIBITED. Any provision of a contract or agreement that waives or
- 6 limits in any way a consumer right described by Sections 541.051,
- 7 541.052, and 541.053 is contrary to public policy and is void and
- 8 <u>unenforceable.</u>
- 9 Sec. 541.055. METHODS FOR SUBMITTING CONSUMER REQUESTS.
- 10 (a) A controller shall establish two or more secure and reliable
- 11 methods to enable consumers to submit a request to exercise their
- 12 consumer rights under this chapter. The methods must take into
- 13 account:
- (1) the ways in which consumers normally interact with
- 15 <u>the controller;</u>
- (2) the necessity for secure and reliable
- 17 communications of those requests; and
- 18 (3) the ability of the controller to authenticate the
- 19 identity of the consumer making the request.
- (b) A controller may not require a consumer to create a new
- 21 account to exercise the consumer's rights under this subchapter but
- 22 may require a consumer to use an existing account.
- (c) Except as provided by Subsection (d), if the controller
- 24 maintains an Internet website, the controller must provide a
- 25 mechanism on the website for consumers to submit requests for
- 26 <u>information required to be disclosed under this chapter.</u>
- 27 (d) A controller that operates exclusively online and has a

- 1 direct relationship with a consumer from whom the controller
- 2 <u>collects personal information is only required to provide an e-mail</u>
- 3 address for the submission of requests described by Subsection (c).
- 4 (e) A consumer may designate another person to serve as the
- 5 consumer's authorized agent and act on the consumer's behalf to opt
- 6 out of the processing of the consumer's personal data under Section
- 7 541.051(b)(5). A consumer may designate an authorized agent using
- 8 <u>a technology</u>, including a link to an Internet website, an Internet
- 9 browser setting or extension, or a global setting on an electronic
- 10 device, that allows the consumer to indicate the consumer's intent
- 11 to opt out of the processing. A controller shall comply with an
- 12 opt-out request received from an authorized agent under this
- 13 subsection if the controller is able to verify, with commercially
- 14 reasonable effort, the identity of the consumer and the authorized
- 15 agent's authority to act on the consumer's behalf. A controller is
- 16 not required to comply with an opt-out request received from an
- 17 authorized agent under this subsection if:
- (1) the authorized agent does not communicate the
- 19 request to the controller in a clear and unambiguous manner;
- (2) the controller is not able to verify, with
- 21 commercially reasonable effort, that the consumer is a resident of
- 22 this state;
- (3) the controller does not possess the technical
- 24 ability to receive the request; or
- 25 (4) the controller does not process similar or
- 26 identical requests the controller receives from consumers for the
- 27 purpose of complying with the laws or regulations of another state.

1	SUBCHAPTER C. CONTROLLER AND PROCESSOR DATA-RELATED DUTIES AND
2	PROHIBITIONS
3	Sec. 541.101. CONTROLLER DUTIES; TRANSPARENCY. (a)
4	<pre>controller:</pre>
5	(1) shall limit the collection of personal data to
6	what is adequate, relevant, and reasonably necessary in relation to
7	the purposes for which that personal data is processed, as
8	disclosed to the consumer; and
9	(2) for purposes of protecting the confidentiality,
10	integrity, and accessibility of personal data, shall establish,
11	implement, and maintain reasonable administrative, technical, and
12	physical data security practices that are appropriate to the volume
13	and nature of the personal data at issue.
14	(b) A controller may not:
15	(1) except as otherwise provided by this chapter,
16	process personal data for a purpose that is neither reasonably
17	necessary to nor compatible with the disclosed purpose for which
18	the personal data is processed, as disclosed to the consumer,
19	unless the controller obtains the consumer's consent;
20	(2) process personal data in violation of state and
21	federal laws that prohibit unlawful discrimination against
22	<pre>consumers;</pre>
23	(3) discriminate against a consumer for exercising any
24	of the consumer rights contained in this chapter, including by
25	denying goods or services, charging different prices or rates for
26	goods or services, or providing a different level of quality of

goods or services to the consumer; or

27

```
1 (4) process the sensitive data of a consumer without
```

- 2 obtaining the consumer's consent, or, in the case of processing the
- 3 sensitive data of a known child, without processing that data in
- 4 accordance with the Children's Online Privacy Protection Act of
- 5 <u>1998 (15 U.S.C. Section 6501 et seq.).</u>
- 6 (c) Subsection (b)(3) may not be construed to require a
- 7 controller to provide a product or service that requires the
- 8 personal data of a consumer that the controller does not collect or
- 9 maintain or to prohibit a controller from offering a different
- 10 price, rate, level, quality, or selection of goods or services to a
- 11 consumer, including offering goods or services for no fee, if the
- 12 consumer has exercised the consumer's right to opt out under
- 13 Section 541.051 or the offer is related to a consumer's voluntary
- 14 participation in a bona fide loyalty, rewards, premium features,
- 15 discounts, or club card program.
- Sec. 541.102. PRIVACY NOTICE. (a) A controller shall
- 17 provide consumers with a reasonably accessible and clear privacy
- 18 notice that includes:
- (1) the categories of personal data processed by the
- 20 controller, including, if applicable, any sensitive data processed
- 21 by the controller;
- 22 (2) the purpose for processing personal data;
- 23 (3) how consumers may exercise their consumer rights
- 24 under Subchapter B, including the process by which a consumer may
- 25 appeal a controller's decision with regard to the consumer's
- 26 <u>request;</u>
- 27 (4) if applicable, the categories of personal data

- 1 that the controller shares with third parties;
- 2 (5) if applicable, the categories of third parties
- 3 with whom the controller shares personal data; and
- 4 (6) a description of the methods required under
- 5 Section 541.055 through which consumers can submit requests to
- 6 exercise their consumer rights under this chapter.
- 7 (b) If a controller engages in the sale of personal data
- 8 that is sensitive data, the controller shall include the following
- 9 notice:
- 10 "NOTICE: This website may sell your sensitive personal data."
- 11 The notice must be posted in the same location and in the same
- 12 manner as the privacy notice described by Subsection (a).
- (c) If a controller engages in the sale of personal data
- 14 that is biometric data, the controller shall include the following
- 15 notice:
- 16 "NOTICE: This website may sell your biometric personal data."
- 17 The notice must be posted in the same location and in the same
- 18 manner as the privacy notice described by Subsection (a).
- 19 Sec. 541.103. SALE OF DATA TO THIRD PARTIES AND PROCESSING
- 20 DATA FOR TARGETED ADVERTISING; DISCLOSURE. If a controller sells
- 21 personal data to third parties or processes personal data for
- 22 targeted advertising, the controller shall clearly and
- 23 conspicuously disclose that process and the manner in which a
- 24 consumer may exercise the right to opt out of that process.
- Sec. 541.104. DUTIES OF PROCESSOR. (a) A processor shall
- 26 adhere to the instructions of a controller and shall assist the
- 27 <u>controller in meeting or complying with the controller's duties or</u>

```
requirements under this chapter, including:
 1
 2
               (1) assisting the controller in responding to consumer
 3
   rights requests submitted under Section 541.051 by using
 4
   appropriate technical and organizational measures, as reasonably
 5
   practicable, taking into account the nature of processing and the
 6
    information available to the processor;
 7
               (2) assisting the controller with regard to complying
   with the requirement relating to the security of processing
 8
   personal data and to the notification of a breach of security of the
 9
   processor's system under Chapter 521, taking into account the
10
11
   nature of processing and the information available to the
12
   processor; and
13
               (3) providing necessary information to enable the
14
    controller to conduct and document data protection assessments
   under Section 541.105.
15
16
          (b) A contract between a controller and a processor shall
17
    govern the processor's data processing procedures with respect to
   processing performed on behalf of the controller. The contract must
18
19
    include:
20
               (1) clear instructions for processing data;
21
               (2)
                    the nature and purpose of processing;
               (3)
                    the type of data subject to processing;
22
23
               (4)
                   the duration of processing;
24
               (5)
                    the rights and obligations of both parties; and
25
               (6)
                    a requirement that the processor shall:
26
                    (A)
                        ensure that each person processing personal
```

data is subject to a duty of confidentiality with respect to the

```
1 <u>data;</u>
```

- 2 (B) at the controller's direction, delete or
- 3 return all personal data to the controller as requested after the
- 4 provision of the service is completed, unless retention of the
- 5 personal data is required by law;
- 6 (C) make available to the controller, on
- 7 reasonable request, all information in the processor's possession
- 8 necessary to demonstrate the processor's compliance with the
- 9 requirements of this chapter;
- (D) allow, and cooperate with, reasonable
- 11 <u>assessments</u> by the controller or the controller's designated
- 12 assessor; and
- (E) engage any subcontractor pursuant to a
- 14 written contract that requires the subcontractor to meet the
- 15 requirements of the processor with respect to the personal data.
- 16 (c) Notwithstanding the requirement described by Subsection
- 17 (b)(6)(D), a processor, in the alternative, may arrange for a
- 18 qualified and independent assessor to conduct an assessment of the
- 19 processor's policies and technical and organizational measures in
- 20 support of the requirements under this chapter using an appropriate
- 21 and accepted control standard or framework and assessment
- 22 procedure. The processor shall provide a report of the assessment
- 23 to the controller on request.
- 24 (d) This section may not be construed to relieve a
- 25 controller or a processor from the liabilities imposed on the
- 26 controller or processor by virtue of its role in the processing
- 27 relationship as described by this chapter.

1	(e) A determination of whether a person is acting as a
2	controller or processor with respect to a specific processing of
3	data is a fact-based determination that depends on the context in
4	which personal data is to be processed. A processor that continues
5	to adhere to a controller's instructions with respect to a specific
6	processing of personal data remains in the role of a processor.
7	Sec. 541.105. DATA PROTECTION ASSESSMENTS. (a) A
8	controller shall conduct and document a data protection assessment
9	of each of the following processing activities involving personal
10	<pre>data:</pre>
11	(1) the processing of personal data for purposes of
12	targeted advertising;
13	(2) the sale of personal data;
14	(3) the processing of personal data for purposes of
15	profiling, if the profiling presents a reasonably foreseeable risk
16	<pre>of:</pre>
17	(A) unfair or deceptive treatment of or unlawful
18	disparate impact on consumers;
19	(B) financial, physical, or reputational injury
20	to consumers;
21	(C) a physical or other intrusion on the solitude
22	or seclusion, or the private affairs or concerns, of consumers, if
23	the intrusion would be offensive to a reasonable person; or
24	(D) other substantial injury to consumers;
25	(4) the processing of sensitive data; and
26	(5) any processing activities involving personal data
27	that present a heightened risk of harm to consumers.

1	(b) A data protection assessment conducted under Subsection
2	<pre>(a) must:</pre>
3	(1) identify and weigh the direct or indirect benefits
4	that may flow from the processing to the controller, the consumer,
5	other stakeholders, and the public, against the potential risks to
6	the rights of the consumer associated with that processing, as
7	mitigated by safeguards that can be employed by the controller to
8	reduce the risks; and
9	(2) factor into the assessment:
10	(A) the use of deidentified data;
11	(B) the reasonable expectations of consumers;
12	(C) the context of the processing; and
13	(D) the relationship between the controller and
14	the consumer whose personal data will be processed.
15	(c) A controller shall make a data protection assessment
16	requested under Section 541.153(b) available to the attorney
17	general pursuant to a civil investigative demand under Section
18	<u>541.153.</u>
19	(d) A data protection assessment is confidential and exempt
20	from public inspection and copying under Chapter 552, Government
21	Code. Disclosure of a data protection assessment in compliance with
22	a request from the attorney general does not constitute a waiver of
23	attorney-client privilege or work product protection with respect
24	to the assessment and any information contained in the assessment.
25	(e) A single data protection assessment may address a
26	comparable set of processing operations that include similar

activities.

27

```
1
         (f) A data protection assessment conducted by a controller
2
   for the purpose of compliance with other laws or regulations may
   constitute compliance with the requirements of this section if the
 3
4
   assessment has a reasonably comparable scope and effect.
         Sec. 541.106. DEIDENTIFIED OR PSEUDONYMOUS DATA. (a) A
5
   controller in possession of deidentified data shall:
6
7
               (1) take reasonable measures to ensure that the data
8
   cannot be associated with an individual;
               (2) publicly commit to maintaining and using
9
   deidentified data without attempting to reidentify the data; and
10
               (3) contractually obligate any recipient of the
11
   deidentified data to comply with the provisions of this chapter.
12
13
         (b) This chapter may not be construed to require a
14
   controller or processor to:
15
              (1) reidentify deidentified data or pseudonymous
   data;
16
17
              (2) maintain data in identifiable form or obtain,
   retain, or access any data or technology for the purpose of allowing
18
   the controller or processor to associate a consumer request with
19
20
   personal data; or
21
               (3) comply with an authenticated consumer rights
22
   request under Section 541.051, if the controller:
23
                    (A) is not reasonably capable of associating the
24
   request with the personal data or it would be unreasonably
   burdensome for the controller to associate the request with the
25
26
   personal data;
```

(B) does not use the personal data to recognize

- 1 or respond to the specific consumer who is the subject of the
- 2 personal data or associate the personal data with other personal
- 3 data about the same specific consumer; and
- 4 (C) does not sell the personal data to any third
- 5 party or otherwise voluntarily disclose the personal data to any
- 6 third party other than a processor, except as otherwise permitted
- 7 by this section.
- 8 (c) The consumer rights under Sections 541.051(b)(1)-(4)
- 9 and controller duties under Section 541.101 do not apply to
- 10 pseudonymous data in cases in which the controller is able to
- 11 demonstrate any information necessary to identify the consumer is
- 12 kept separately and is subject to effective technical and
- 13 organizational controls that prevent the controller from accessing
- 14 the information.
- 15 (d) A controller that discloses pseudonymous data or
- 16 <u>deidentified data shall exercise reasonable oversight to monitor</u>
- 17 compliance with any contractual commitments to which the
- 18 pseudonymous data or deidentified data is subject and shall take
- 19 appropriate steps to address any breach of the contractual
- 20 commitments.
- Sec. 541.107. REQUIREMENTS FOR SMALL BUSINESSES. (a) A
- 22 person described by Section 541.002(a)(3) may not engage in the
- 23 sale of personal data that is sensitive data without receiving
- 24 prior consent from the consumer.
- (b) A person who violates this section is subject to the
- 26 penalty under Section 541.155.

1	SUBCHAPTER D. ENFORCEMENT
2	Sec. 541.151. ENFORCEMENT AUTHORITY EXCLUSIVE. The
3	attorney general has exclusive authority to enforce this chapter.
4	Sec. 541.152. INTERNET WEBSITE AND COMPLAINT MECHANISM.
5	The attorney general shall post on the attorney general's Internet
6	website:
7	(1) information relating to:
8	(A) the responsibilities of a controller under
9	Subchapters B and C;
10	(B) the responsibilities of a processor under
11	Subchapter C; and
12	(C) a consumer's rights under Subchapter B; and
13	(2) an online mechanism through which a consumer may
14	submit a complaint under this chapter to the attorney general.
15	Sec. 541.153. INVESTIGATIVE AUTHORITY. (a) If the
16	attorney general has reasonable cause to believe that a person has
17	engaged in or is engaging in a violation of this chapter, the
18	attorney general may issue a civil investigative demand. The
19	procedures established for the issuance of a civil investigative
20	demand under Section 15.10 apply to the same extent and manner to
21	the issuance of a civil investigative demand under this section.
22	(b) The attorney general may request, pursuant to a civil
23	investigative demand issued under Subsection (a), that a controller
24	disclose any data protection assessment that is relevant to an
25	investigation conducted by the attorney general. The attorney
26	general may evaluate the data protection assessment for compliance
27	with the requirements set forth in Sections 541.101, 541.102, and

```
1 541.103.
```

- 2 Sec. 541.154. NOTICE OF VIOLATION OF CHAPTER; OPPORTUNITY
- 3 TO CURE. Before bringing an action under Section 541.155, the
- 4 attorney general shall notify a person in writing, not later than
- 5 the 30th day before bringing the action, identifying the specific
- 6 provisions of this chapter the attorney general alleges have been
- 7 or are being violated. The attorney general may not bring an action
- 8 against the person if:
- 9 (1) within the 30-day period, the person cures the
- 10 identified violation; and
- 11 (2) the person provides the attorney general a written
- 12 statement that the person:
- (A) cured the alleged violation;
- 14 (B) notified the consumer that the consumer's
- 15 privacy violation was addressed, if the consumer's contact
- 16 information has been made available to the person;
- (C) provided supportive documentation to show
- 18 how the privacy violation was cured; and
- (D) made changes to internal policies, if
- 20 necessary, to ensure that no such further violations will occur.
- Sec. 541.155. CIVIL PENALTY; INJUNCTION. (a) A person who
- 22 violates this chapter following the cure period described by
- 23 Section 541.154 or who breaches a written statement provided to the
- 24 attorney general under that section is liable for a civil penalty in
- an amount not to exceed \$7,500 for each violation.
- 26 (b) The attorney general may bring an action in the name of
- 27 this state to:

- 1 (1) recover a civil penalty under this section;
- 2 (2) restrain or enjoin the person from violating this
- 3 chapter; or
- 4 (3) recover the civil penalty and seek injunctive
- 5 relief.
- 6 (c) The attorney general may recover reasonable attorney's
- 7 fees and other reasonable expenses incurred in investigating and
- 8 bringing an action under this section.
- 9 (d) The attorney general shall deposit a civil penalty
- 10 collected under this section in accordance with Section 402.007,
- 11 Government Code.
- Sec. 541.156. DEFENSE TO LIABILITY. (a) A controller may
- 13 assert a defense to liability under Section 541.155 if more than 60
- 14 percent of the controller's revenue is generated by consumers,
- 15 persons, or other entities in this state.
- 16 (b) This section expires September 1, 2024.
- Sec. 541.157. NO PRIVATE RIGHT OF ACTION. This chapter may
- 18 not be construed as providing a basis for, or being subject to, a
- 19 private right of action for a violation of this chapter or any other
- 20 <u>law.</u>
- 21 SUBCHAPTER E. CONSTRUCTION OF CHAPTER; EXEMPTIONS FOR CERTAIN USES
- 22 <u>OF CONSUMER PERSONAL DATA</u>
- Sec. 541.201. CONSTRUCTION OF CHAPTER. (a) This chapter
- 24 may not be construed to restrict a controller's or processor's
- 25 ability to:
- 26 (1) comply with federal, state, or local laws, rules,
- 27 or regulations;

- 1 (2) comply with a civil, criminal, or regulatory
- 2 inquiry, investigation, subpoena, or summons by federal, state,
- 3 local, or other governmental authorities;
- 4 (3) investigate, establish, exercise, prepare for, or
- 5 defend legal claims;
- 6 (4) provide a product or service specifically
- 7 requested by a consumer or the parent or guardian of a child,
- 8 perform a contract to which the consumer is a party, including
- 9 fulfilling the terms of a written warranty, or take steps at the
- 10 request of the consumer before entering into a contract;
- 11 (5) take immediate steps to protect an interest that
- 12 is essential for the life or physical safety of the consumer or of
- 13 another individual and in which the processing cannot be manifestly
- 14 based on another legal basis;
- 15 (6) prevent, detect, protect against, or respond to
- 16 security incidents, identity theft, fraud, harassment, malicious
- 17 or deceptive activities, or any illegal activity;
- 18 (7) preserve the integrity or security of systems or
- 19 investigate, report, or prosecute those responsible for breaches of
- 20 system security;
- 21 (8) engage in public or peer-reviewed scientific or
- 22 statistical research in the public interest that adheres to all
- 23 other applicable ethics and privacy laws and is approved,
- 24 monitored, and governed by an institutional review board or similar
- 25 independent oversight entity that determines:
- 26 (A) if the deletion of the information is likely
- 27 to provide substantial benefits that do not exclusively accrue to

```
1 the controller;
```

- 2 (B) whether the expected benefits of the research
- 3 outweigh the privacy risks; and
- 4 (C) if the controller has implemented reasonable
- 5 safeguards to mitigate privacy risks associated with research,
- 6 including any risks associated with reidentification; or
- 7 (9) assist another controller, processor, or third
- 8 party with any of the requirements under this subsection.
- 9 (b) This chapter may not be construed to prevent a
- 10 controller or processor from providing personal data concerning a
- 11 consumer to a person covered by an evidentiary privilege under the
- 12 laws of this state as part of a privileged communication.
- 13 (c) This chapter may not be construed as imposing a
- 14 requirement on controllers and processors that adversely affects
- 15 the rights or freedoms of any person, including the right of free
- 16 speech.
- 17 (d) This chapter may not be construed as requiring a
- 18 controller, processor, third party, or consumer to disclose a trade
- 19 secret.
- Sec. 541.202. COLLECTION, USE, OR RETENTION OF DATA FOR
- 21 CERTAIN PURPOSES. (a) The requirements imposed on controllers and
- 22 processors under this chapter may not restrict a controller's or
- 23 processor's ability to collect, use, or retain data to:
- 24 (1) conduct internal research to develop, improve, or
- 25 repair products, services, or technology;
- 26 (2) effect a product recall;
- 27 (3) identify and repair technical errors that impair

```
1
   existing or intended functionality; or
2
               (4) perform internal operations that:
3
                    (A) are reasonably aligned with the expectations
4
   of the consumer;
5
                    (B) are reasonably anticipated based on the
6
   consumer's existing relationship with the controller; or
7
                    (C) are otherwise compatible with processing
   data in furtherance of the provision of a product or service
8
   specifically requested by a consumer or the performance of a
9
10
   contract to which the consumer is a party.
11
         (b) A requirement imposed on a controller or processor under
   this chapter does not apply if compliance with the requirement by
12
   the controller or processor, as applicable, would violate an
13
   evidentiary privilege under the laws of this state.
14
         Sec. 541.203. DISCLOSURE OF PERSONAL DATA TO THIRD-PARTY
15
16
   CONTROLLER OR PROCESSOR. (a) A controller or processor that
17
   discloses personal data to a third-party controller or processor,
   in compliance with the requirements of this chapter, does not
18
   violate this chapter if the third-party controller or processor
19
20
   that receives and processes that personal data is in violation of
21
   this chapter, provided that, at the time of the data's disclosure,
22
   the disclosing controller or processor did not have actual
23
   knowledge that the recipient intended to commit a violation.
         (b) A third-party controller or processor receiving
24
```

26

27

personal data from a controller or processor in compliance with the

requirements of this chapter does not violate this chapter for the

transgressions of the controller or processor from which the

- 1 third-party controller or processor receives the personal data.
- 2 Sec. 541.204. PROCESSING OF CERTAIN PERSONAL DATA BY
- 3 CONTROLLER OR OTHER PERSON. (a) Personal data processed by a
- 4 controller under this subchapter may not be processed for any
- 5 purpose other than a purpose listed in this subchapter unless
- 6 otherwise allowed by this chapter. Personal data processed by a
- 7 controller under this subchapter may be processed to the extent
- 8 that the processing of the data is:
- 9 (1) reasonably necessary and proportionate to the
- 10 purposes listed in this subchapter; and
- 11 (2) adequate, relevant, and limited to what is
- 12 necessary in relation to the specific purposes listed in this
- 13 subchapter.
- (b) Personal data collected, used, or retained under
- 15 Section 541.202(a) must, where applicable, take into account the
- 16 nature and purpose of such collection, use, or retention. The
- 17 personal data described by this subsection is subject to reasonable
- 18 administrative, technical, and physical measures to protect the
- 19 confidentiality, integrity, and accessibility of the personal data
- 20 and to reduce reasonably foreseeable risks of harm to consumers
- 21 relating to the collection, use, or retention of personal data.
- (c) A controller that processes personal data under an
- 23 exemption in this subchapter bears the burden of demonstrating that
- 24 the processing of the personal data qualifies for the exemption and
- 25 complies with the requirements of Subsections (a) and (b).
- 26 (d) The processing of personal data by an entity for the
- 27 purposes described by Section 541.201 does not solely make the

- 1 entity a controller with respect to the processing of the data.
- 2 Sec. 541.205. LOCAL PREEMPTION. This chapter supersedes
- 3 and preempts any ordinance, resolution, rule, or other regulation
- 4 adopted by a political subdivision regarding the processing of
- 5 personal data by a controller or processor.
- 6 SECTION 3. (a) The Department of Information Resources,
- 7 under the management of the chief privacy officer, shall review the
- 8 implementation of the requirements of Chapter 541, Business &
- 9 Commerce Code, as added by this Act.
- 10 (b) Not later than September 1, 2024, the Department of
- 11 Information Resources shall create an online portal available on
- 12 the department's Internet website for members of the public to
- 13 provide feedback and recommend changes to Chapter 541, Business &
- 14 Commerce Code, as added by this Act. The online portal must remain
- 15 open for receiving feedback from the public for at least 90 days.
- 16 (c) Not later than January 1, 2025, the Department of
- 17 Information Resources shall make available to the public a report
- 18 detailing the status of the implementation of the requirements of
- 19 Chapter 541, Business & Commerce Code, as added by this Act, and any
- 20 recommendations to the legislature regarding changes to that law.
- 21 (d) This section expires September 1, 2025.
- 22 SECTION 4. Data protection assessments required to be
- 23 conducted under Section 541.105, Business & Commerce Code, as added
- 24 by this Act, apply only to processing activities generated after
- 25 the effective date of this Act and are not retroactive.
- SECTION 5. Not later than March 1, 2024, the attorney
- 27 general shall post the information and online mechanism required by

- 1 Section 541.152, Business & Commerce Code, as added by this Act.
- 2 SECTION 6. The provisions of this Act are hereby declared
- 3 severable, and if any provision of this Act or the application of
- 4 such provision to any person or circumstance is declared invalid
- 5 for any reason, such declaration shall not affect the validity of
- 6 the remaining portions of this Act.
- 7 SECTION 7. (a) Except as provided by Subsection (b) of this
- 8 section, this Act takes effect March 1, 2024.
- 9 (b) Section 541.055(e), Business & Commerce Code, as added
- 10 by this Act, takes effect January 1, 2025.

Third Reading

ADOPTED MAY 10 2023

Latey Saw Secretary of the Senate

FLOOR AMENDMENT NO. /

BY Bull

1 Amend C.S.H.B. No. 4 (senate committee report), in SECTION 2

2 of the bill (page 13, line 25), by striking "September 1, 2024"

3 and substituting "January 1, 2025".

FLOOR AMENDMENT NO. \_\_\_\_

MAY 10 2028 Langer Langer Langer Secretary of the Senate

- 1 Amend C.S.H.B. No. 4 (senate committee printing) in SECTION 2
- 2 of the bill as follows:
- 3 (1) In added Section 541.001(30), Business & Commerce Code
- 4 (page 4, line 42), strike "the executive" and substitute "any".
- 5 (2) In added Sections 541.102(b) and (c), Business &
- 6 Commerce Code (page 9, lines 50 through 61), strike "This website"
- 7 in each place it appears and substitute " $\underline{We}$ ".

#### FISCAL NOTE, 88TH LEGISLATIVE REGULAR SESSION

May 11, 2023

**TO:** Honorable Dade Phelan, Speaker of the House, House of Representatives

FROM: Jerry McGinty, Director, Legislative Budget Board

IN RE: HB4 by Capriglione (Relating to the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities; imposing a civil penalty.), As Passed 2nd House

**Estimated Two-year Net Impact to General Revenue Related Funds** for HB4, As Passed 2nd House: a negative impact of (\$7,536,192) through the biennium ending August 31, 2025.

The bill would make no appropriation but could provide the legal basis for an appropriation of funds to implement the provisions of the bill.

## **General Revenue-Related Funds, Five- Year Impact:**

Fiscal Year	Probable Net Positive/(Negative) Impact to General Revenue Related Funds	
2024	(\$5,580,216)	
2025	(\$1,955,976)	
2026	(\$1,705,976)	
2027	(\$1,705,976)	
2028	(\$1,705,976)	

#### All Funds, Five-Year Impact:

Fiscal Year	Probable Savings/(Cost) from General Revenue Fund 1	Change in Number of State Employees from FY 2023
2024	(\$5,580,216)	12.0
2025	(\$1,955,976)	12.0
2026	(\$1,705,976)	12.0
2027	(\$1,705,976)	12.0
2028	(\$1,705,976)	12.0

# Fiscal Analysis

The bill amends the Business & Commerce Code by adding Chapter 541, The Texas Data Privacy and Security Act (TDPSA), to address the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities. TDPSA provides consumers residing in Texas with certain rights regarding personal data. These include: the right to request confirmation of whether a controller is processing the consumer's personal data; the right to correct inaccuracies in personal data; the right to delete personal data provided by or obtained about the consumer; the right to obtain data (if feasible) in a portable, readily usable format so that the consumer may transmit it to another controller; and the right to opt out of the processing of

personal data for purposes of targeted advertising, sale of personal data, or profiling "in furtherance of a decision that produces a legal or similarly significant effect."

TDPSA would require that controllers provide consumers with notice when they decline to act regarding a consumer's request and to provide justification for declining to act and additionally, to provide instructions on how to appeal the decision. Controllers must provide information in response to a consumer request free of charge, up to twice annually per consumer - unless the request is unfounded, excessive, or repetitive, in which case the consumer may be charged a reasonable fee to cover administrative costs. Controllers must establish a process for consumers to appeal their decisions. If the controller denies an appeal, the controller must provide the consumer with an online mechanism, if available, or another method to contact the OAG to submit a complaint.

The bill would require that certain specific provisions be included in contracts between controllers and processors. The Office of the Attorney General (OAG) has exclusive authority to enforce the provisions of this bill and may obtain injunctive relief, civil penalties of up to \$7,500 per violation, and reasonable attorneys' fees and investigative expenses. Penalties recovered are to be deposited in the general revenue fund.

If the OAG has "reasonable cause to believe" that a person has engaged in, is engaging in, or is about to engage in a violation of this bill, the OAG may issue a civil investigative demand (CID). The bill specifically authorizes the OAG to issue CIDs to controllers requesting relevant data protection assessments and requires controllers to provide those to the OAG. These assessments are confidential and exempt from the Texas Public Information Act, and disclosure to the OAG is not waiver of attorney client or work product privilege regarding information in the assessment. The procedure for CIDs is those established under Texas Business & Commerce Code, Section 15.10.

The bill would require that the OAG post on its website information relating to the responsibilities of a controller and a processor, as well as an online mechanism through which a consumer can submit a complaint TDSPA to the OAG.

Before bringing an action, the OAG is required to provide written notice of specific violations. If the person cures the identified violation within 30 days and provides a written statement that the person cured the violation, notified the consumer that the consumer's privacy violation was addressed, provided supportive documentation to show how the privacy violation was cured, and made changes to internal policies to ensure no further violations will occur, the OAG may not bring an action. Violations of the bill following the 30-day cure period and breaches of the written statement provided to the OAG are subject to enforcement actions including a civil penalty of up to \$7,500 per violation.

## Methodology

The OAG estimates that enactment of the bill will generate an increased number of inquiries from lawmakers, business and legal communities, privacy advocates, the general public, and the media regarding the implementation and enforcement of this bill. The OAG indicates that additional resources would be needed to undertake enforcement efforts and would require additional resources for receiving and processing privacy rights complaints and for the investigation and litigation of cases including the retention of consulting experts. Enforcement would require analyzing complaints; identifying issues and alleged violations of the law; issuing civil investigative demands; reviewing and evaluating data protection assessments; conducting factual and legal research to assess violations and viability of potential claims and defenses; retaining and conferring with consulting experts; and litigation activities including discovery, motions practice, preparing for trial, trial, and appeal.

OAG staff would need to devote time to provide feedback to DIR as it prepares a legislatively mandated report regarding the implementation of this bill and recommendations regarding the changes to the law.

The OAG indicates that they would need twelve additional FTEs to handle the anticipated increase in workload resulting from this bill. These additional FTEs include two Assistant Attorney General (AAG) II, two AAG IV, one AAG VI, one Compliance Analyst II, one Data Analyst II, one Data Analyst V, one Legal Assistant I, one Legal Assistant III, one Programmer VI, and one System Administrator V to handle the increased workload. The FTE costs are \$1,520,760 in fiscal year 2024 and \$1,460,370 each fiscal year thereafter. Costs include salary,

general operating, travel, capital equipment (technology related and furniture), and benefits.

The Office of Court Administration, Commission on Judicial Conduct, Comptroller of Public Accounts, Department of Information Resources, Bond Review Board, Texas Medical Board, Health & Human Services Commission, Department of Transportation, Texas A&M University System, UT University System, Higher Education Coordinating Board, and Alamo Community College all anticipate no significant fiscal impact from the provisions of the bill. The Comptroller of Public Accounts indicates that the amounts and timing of any penalty revenue are unknown, but is unlikely to be significant.

#### **Technology**

The technology impact includes one-time costs of \$3,563,850 in fiscal year 2024 for the creation of the system, project management costs of \$250,000 each year in fiscal years 2024 and 2025, and a recurring cost in each fiscal year of \$245,606. One-time costs include system development, project management costs, standard laptop, software, printer, and telecom/voicemail. Annual recurring charges cover consulting costs for technology experts, data center services, and voice line.

# **Local Government Impact**

No significant fiscal implication to units of local government is anticipated.

Source Agencies: 212 Office of Court Administration, Texas Judicial Council, 242 State Commission on Judicial Conduct,

302 Office of the Attorney General, 304 Comptroller of Public Accounts, 313 Department of Information Resources, 352 Bond Review Board, 503 Texas Medical Board, 529 Health and Human Services Commission, 601 Department of Transportation, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration, 781 Higher

**Education Coordinating Board** 

LBB Staff: JMc, CMA, HGR, SMAT, SZ, LCO

## FISCAL NOTE, 88TH LEGISLATIVE REGULAR SESSION

May 7, 2023

TO: Honorable Bryan Hughes, Chair, Senate Committee on State Affairs

FROM: Jerry McGinty, Director, Legislative Budget Board

IN RE: HB4 by Capriglione (relating to the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities; imposing a civil penalty.), Committee Report 2nd House, Substituted

Estimated Two-year Net Impact to General Revenue Related Funds for HB4, Committee Report 2nd House, Substituted: a negative impact of (\$7,536,192) through the biennium ending August 31, 2025.

The bill would make no appropriation but could provide the legal basis for an appropriation of funds to implement the provisions of the bill.

# General Revenue-Related Funds, Five- Year Impact:

Fiscal Year	Probable Net Positive/(Negative) Impact to General Revenue Related Funds	
2024	(\$5,580,216)	
2025	(\$1,955,976)	
2026	(\$1,705,976)	
2027	(\$1,705,976)	
2028	(\$1,705,976)	

Fiscal Year	Probable Savings/(Cost) from General Revenue Fund 1	Change in Number of State Employees from FY 2023
2024	(\$5,580,216)	12.0
2025	(\$1,955,976)	12.0
2026	(\$1,705,976)	12.0
2027	(\$1,705,976)	12.0
2028	(\$1,705,976)	12.0

The bill amends the Business & Commerce Code by adding Chapter 541, The Texas Data Privacy and Security Act (TDPSA), to address the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities. TDPSA provides consumers residing in Texas with certain rights regarding personal data. These include: the right to request confirmation of whether a controller is processing the consumer's personal data; the right to correct inaccuracies in personal data; the right to delete personal data provided by or obtained about the consumer; the right to obtain data (if feasible) in a portable, readily usable format so that the consumer may transmit it to another controller; and the right to opt out of the processing of personal data for purposes of targeted advertising, sale of personal data, or profiling "in furtherance of a decision that produces a legal or similarly significant effect."

TDPSA would require that controllers provide consumers with notice when they decline to act regarding a consumer's request and to provide justification for declining to act and additionally, to provide instructions on how to appeal the decision. Controllers must provide information in response to a consumer request free of charge, up to twice annually per consumer - unless the request is unfounded, excessive, or repetitive, in which case the consumer may be charged a reasonable fee to cover administrative costs. Controllers must establish a process for consumers to appeal their decisions. If the controller denies an appeal, the controller must provide the consumer with an online mechanism, if available, or another method to contact the OAG to submit a complaint.

The bill would require that certain specific provisions be included in contracts between controllers and processors. The Office of the Attorney General (OAG) has exclusive authority to enforce the provisions of this bill and may obtain injunctive relief, civil penalties of up to \$7,500 per violation, and reasonable attorneys' fees and investigative expenses. Penalties recovered are to be deposited in the general revenue fund.

If the OAG has "reasonable cause to believe" that a person has engaged in, is engaging in, or is about to engage in a violation of this bill, the OAG may issue a civil investigative demand (CID). The bill specifically authorizes the OAG to issue CIDs to controllers requesting relevant data protection assessments and requires controllers to provide those to the OAG. These assessments are confidential and exempt from the Texas Public Information Act, and disclosure to the OAG is not waiver of attorney client or work product privilege regarding information in the assessment. The procedure for CIDs is those established under Texas Business & Commerce Code, Section 15.10.

The bill would require that the OAG post on its website information relating to the responsibilities of a controller and a processor, as well as an online mechanism through which a consumer can submit a complaint TDSPA to the OAG.

Before bringing an action, the OAG is required to provide written notice of specific violations. If the person cures the identified violation within 30 days and provides a written statement that the person cured the violation, notified the consumer that the consumer's privacy violation was addressed, provided supportive documentation to show how the privacy violation was cured, and made changes to internal policies to ensure no further violations will occur, the OAG may not bring an action. Violations of the bill following the 30-day cure period and breaches of the written statement provided to the OAG are subject to enforcement actions including a civil penalty of up to \$7,500 per violation.

## Methodology

The OAG estimates that enactment of the bill will generate an increased number of inquiries from lawmakers, business and legal communities, privacy advocates, the general public, and the media regarding the implementation and enforcement of this bill. The OAG indicates that additional resources would be needed to undertake enforcement efforts and would require additional resources for receiving and processing privacy rights complaints and for the investigation and litigation of cases including the retention of consulting experts. Enforcement would require analyzing complaints; identifying issues and alleged violations of the law; issuing civil investigative demands; reviewing and evaluating data protection assessments; conducting factual and legal research to assess violations and viability of potential claims and defenses; retaining and conferring with consulting experts; and litigation activities including discovery, motions practice, preparing for trial, trial, and appeal.

OAG staff would need to devote time to provide feedback to DIR as it prepares a legislatively mandated report regarding the implementation of this bill and recommendations regarding the changes to the law.

The OAG indicates that they would need twelve additional FTEs to handle the anticipated increase in workload resulting from this bill. These additional FTEs include two Assistant Attorney General (AAG) II, two AAG IV, one AAG VI, one Compliance Analyst II, one Data Analyst II, one Data Analyst V, one Legal Assistant I, one Legal Assistant III, one Programmer VI, and one System Administrator V to handle the increased workload. The FTE costs are \$1,520,760 in fiscal year 2024 and \$1,460,370 each fiscal year thereafter. Costs include salary, general operating, travel, capital equipment (technology related and furniture), and benefits.

The Office of Court Administration, Commission on Judicial Conduct, Comptroller of Public Accounts, Department of Information Resources, Bond Review Board, Texas Medical Board, Health & Human Services Commission, Department of Transportation, Texas A&M University System, UT University System, Higher Education Coordinating Board, and Alamo Community College all anticipate no significant fiscal impact from the provisions of the bill. The Comptroller of Public Accounts indicates that the amounts and timing of any penalty revenue are unknown, but is unlikely to be significant.

#### **Technology**

The technology impact includes one-time costs of \$3,563,850 in fiscal year 2024 for the creation of the system, project management costs of \$250,000 each year in fiscal years 2024 and 2025, and a recurring cost in each fiscal year of \$245,606. One-time costs include system development, project management costs, standard laptop, software, printer, and telecom/voicemail. Annual recurring charges cover consulting costs for technology experts, data center services, and voice line.

## **Local Government Impact**

No significant fiscal implication to units of local government is anticipated.

Source Agencies: 212 Office of Court Administration, Texas Judicial Council, 242 State Commission on Judicial Conduct,

302 Office of the Attorney General, 304 Comptroller of Public Accounts, 313 Department of Information Resources, 352 Bond Review Board, 503 Texas Medical Board, 529 Health and Human Services Commission, 601 Department of Transportation, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration, 781 Higher

**Education Coordinating Board** 

LBB Staff: JMc, SMAT, HGR, SZ, LCO

#### FISCAL NOTE, 88TH LEGISLATIVE REGULAR SESSION

May 2, 2023

TO: Honorable Bryan Hughes, Chair, Senate Committee on State Affairs

FROM: Jerry McGinty, Director, Legislative Budget Board

IN RE: HB4 by Capriglione (Relating to the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities; imposing a civil penalty.), As Engrossed

**Estimated Two-year Net Impact to General Revenue Related Funds** for HB4, As Engrossed : a negative impact of (\$7,536,192) through the biennium ending August 31, 2025.

The bill would make no appropriation but could provide the legal basis for an appropriation of funds to implement the provisions of the bill.

## General Revenue-Related Funds, Five- Year Impact:

Fiscal Year	Probable Net Positive/(Negative) Impact to General Revenue Related Funds	
2024	(\$5,580,216)	
2025	(\$1,955,976)	
2026	(\$1,705,976)	
2027	(\$1,705,976)	
2028	(\$1,705,976)	

Fiscal Year	Probable Savings/(Cost) from General Revenue Fund	Change in Number of State Employees from FY 2023
2024	(\$5,580,216)	12.0
2025	(\$1,955,976)	12.0
2026	(\$1,705,976)	12.0
2027	(\$1,705,976)	12.0
2028	(\$1,705,976)	12.0

The bill amends the Business & Commerce Code by adding Chapter 541, The Texas Data Privacy and Security Act (TDPSA), to address the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities. TDPSA provides consumers residing in Texas with certain rights regarding personal data. These include: the right to request confirmation of whether a controller is processing the consumer's personal data; the right to correct inaccuracies in personal data; the right to delete personal data provided by or obtained about the consumer; the right to obtain data (if feasible) in a portable, readily usable format so that the consumer may transmit it to another controller; and the right to opt out of the processing of personal data for purposes of targeted advertising, sale of personal data, or profiling "in furtherance of a decision that produces a legal or similarly significant effect."

TDPSA would require that controllers provide consumers with notice when they decline to act regarding a consumer's request and to provide justification for declining to act and additionally, to provide instructions on how to appeal the decision. Controllers must provide information in response to a consumer request free of charge, up to twice annually per consumer - unless the request is unfounded, excessive, or repetitive, in which case the consumer may be charged a reasonable fee to cover administrative costs. Controllers must establish a process for consumers to appeal their decisions. If the controller denies an appeal, the controller must provide the consumer with an online mechanism, if available, or another method to contact the OAG to submit a complaint.

The bill would require that certain specific provisions be included in contracts between controllers and processors. The Office of the Attorney General (OAG) has exclusive authority to enforce the provisions of this bill and may obtain injunctive relief, civil penalties of up to \$7,500 per violation, and reasonable attorneys' fees and investigative expenses. Penalties recovered are to be deposited in the general revenue fund.

If the OAG has "reasonable cause to believe" that a person has engaged in, is engaging in, or is about to engage in a violation of this bill, the OAG may issue a civil investigative demand (CID). The bill specifically authorizes the OAG to issue CIDs to controllers requesting relevant data protection assessments and requires controllers to provide those to the OAG. These assessments are confidential and exempt from the Texas Public Information Act, and disclosure to the OAG is not waiver of attorney client or work product privilege regarding information in the assessment. The procedure for CIDs is those established under Texas Business & Commerce Code, Section 15.10.

The bill would require that the OAG post on its website information relating to the responsibilities of a controller and a processor, as well as an online mechanism through which a consumer can submit a complaint TDSPA to the OAG.

Before bringing an action, the OAG is required to provide written notice of specific violations. If the person cures the identified violation within 30 days and provides a written statement that the person cured the violation, notified the consumer that the consumer's privacy violation was addressed, provided supportive documentation to show how the privacy violation was cured, and made changes to internal policies to ensure no further violations will occur, the OAG may not bring an action. Violations of the bill following the 30-day cure period and breaches of the written statement provided to the OAG are subject to enforcement actions including a civil penalty of up to \$7,500 per violation.

# Methodology

The OAG estimates that enactment of the bill will generate an increased number of inquiries from lawmakers, business and legal communities, privacy advocates, the general public, and the media regarding the implementation and enforcement of this bill. The OAG indicates that additional resources would be needed to undertake enforcement efforts and would require additional resources for receiving and processing privacy rights complaints and for the investigation and litigation of cases including the retention of consulting experts. Enforcement would require analyzing complaints; identifying issues and alleged violations of the law; issuing civil investigative demands; reviewing and evaluating data protection assessments; conducting factual and legal research to assess violations and viability of potential claims and defenses; retaining and conferring with consulting experts; and litigation activities including discovery, motions practice, preparing for trial, trial, and appeal.

OAG staff would need to devote time to provide feedback to DIR as it prepares a legislatively mandated report regarding the implementation of this bill and recommendations regarding the changes to the law.

The OAG indicates that they would need twelve additional FTEs to handle the anticipated increase in workload resulting from this bill. These additional FTEs include two Assistant Attorney General (AAG) II, two AAG IV, one AAG VI, one Compliance Analyst II, one Data Analyst II, one Data Analyst V, one Legal Assistant I, one Legal Assistant III, one Programmer VI, and one System Administrator V to handle the increased workload. The FTE costs are \$1,520,760 in fiscal year 2024 and \$1,460,370 each fiscal year thereafter. Costs include salary, general operating, travel, capital equipment (technology related and furniture), and benefits.

The Office of Court Administration, Commission on Judicial Conduct, Comptroller of Public Accounts, Department of Information Resources, Bond Review Board, Texas Medical Board, Health & Human Services Commission, Department of Transportation, Texas A&M University System, UT University System, Higher Education Coordinating Board, and Alamo Community College all anticipate no significant fiscal impact from the provisions of the bill. The Comptroller of Public Accounts indicates that the amounts and timing of any penalty revenue are unknown, but is unlikely to be significant.

#### **Technology**

The technology impact includes one-time costs of \$3,563,850 in fiscal year 2024 for the creation of the system, project management costs of \$250,000 each year in fiscal years 2024 and 2025, and a recurring cost in each fiscal year of \$245,606. One-time costs include system development, project management costs, standard laptop, software, printer, and telecom/voicemail. Annual recurring charges cover consulting costs for technology experts, data center services, and voice line.

## **Local Government Impact**

No significant fiscal implication to units of local government is anticipated.

Source Agencies: 212 Office of Court Administration, Texas Judicial Council, 242 State Commission on Judicial Conduct,

302 Office of the Attorney General, 304 Comptroller of Public Accounts, 313 Department of Information Resources, 352 Bond Review Board, 503 Texas Medical Board, 529 Health and Human Services Commission, 601 Department of Transportation, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration, 781 Higher

**Education Coordinating Board** 

LBB Staff: JMc, SMAT, SZ, LCO, HGR

#### FISCAL NOTE, 88TH LEGISLATIVE REGULAR SESSION

#### March 22, 2023

TO: Honorable Oscar Longoria, Chair, House Committee on Business & Industry

FROM: Jerry McGinty, Director, Legislative Budget Board

IN RE: HB4 by Capriglione (relating to the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities; imposing a civil penalty.), Committee Report 1st House, Substituted

Estimated Two-year Net Impact to General Revenue Related Funds for HB4, Committee Report 1st House, Substituted: a negative impact of (\$7,536,192) through the biennium ending August 31, 2025.

The bill would make no appropriation but could provide the legal basis for an appropriation of funds to implement the provisions of the bill.

#### General Revenue-Related Funds, Five- Year Impact:

Fiscal Year	Probable Net Positive/(Negative) Impact to General Revenue Related Funds	
2024	(\$5,580,216)	
2025	(\$1,955,976)	
2026	(\$1,705,976)	
2027	(\$1,705,976)	
2028	(\$1,705,976)	

Fiscal Year	Probable Savings/(Cost) from General Revenue Fund 1	Change in Number of State Employees from FY 2023
2024	(\$5,580,216)	12.0
2025	(\$1,955,976)	12.0
2026	(\$1,705,976)	12.0
2027	(\$1,705,976)	12.0
2028	(\$1,705,976)	12.0

The bill amends the Business & Commerce Code by adding Chapter 541, The Texas Data Privacy and Security Act (TDPSA), to address the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities. TDPSA provides consumers residing in Texas with certain rights regarding personal data. These include: the right to request confirmation of whether a controller is processing the consumer's personal data; the right to correct inaccuracies in personal data; the right to delete personal data provided by or obtained about the consumer; the right to obtain data (if feasible) in a portable, readily usable format so that the consumer may transmit it to another controller; and the right to opt out of the processing of personal data for purposes of targeted advertising, sale of personal data, or profiling "in furtherance of a decision that produces a legal or similarly significant effect."

TDPSA would require that controllers provide consumers with notice when they decline to act regarding a consumer's request and to provide justification for declining to act and additionally, to provide instructions on how to appeal the decision. Controllers must provide information in response to a consumer request free of charge, up to twice annually per consumer - unless the request is unfounded, excessive, or repetitive, in which case the consumer may be charged a reasonable fee to cover administrative costs. Controllers must establish a process for consumers to appeal their decisions. If the controller denies an appeal, the controller must provide the consumer with an online mechanism, if available, or another method to contact the OAG to submit a complaint.

The bill would require that certain specific provisions be included in contracts between controllers and processors. The Office of the Attorney General (OAG) has exclusive authority to enforce the provisions of this bill and may obtain injunctive relief, civil penalties of up to \$7,500 per violation, and reasonable attorneys' fees and investigative expenses. Penalties recovered are to be deposited in the general revenue fund.

If the OAG has "reasonable cause to believe" that a person has engaged in, is engaging in, or is about to engage in a violation of this bill, the OAG may issue a civil investigative demand (CID). The bill specifically authorizes the OAG to issue CIDs to controllers requesting relevant data protection assessments and requires controllers to provide those to the OAG. These assessments are confidential and exempt from the Texas Public Information Act, and disclosure to the OAG is not waiver of attorney client or work product privilege regarding information in the assessment. The procedure for CIDs is those established under Texas Business & Commerce Code, Section 15.10.

The bill would require that the OAG post on its website information relating to the responsibilities of a controller and a processor, as well as an online mechanism through which a consumer can submit a complaint TDSPA to the OAG.

Before bringing an action, the OAG is required to provide written notice of specific violations. If the person cures the identified violation within 30 days and provides a written statement that the person cured the violation, notified the consumer that the consumer's privacy violation was addressed, provided supportive documentation to show how the privacy violation was cured, and made changes to internal policies to ensure no further violations will occur, the OAG may not bring an action. Violations of the bill following the 30-day cure period and breaches of the written statement provided to the OAG are subject to enforcement actions including a civil penalty of up to \$7,500 per violation.

# Methodology

The OAG estimates that enactment of the bill will generate an increased number of inquiries from lawmakers, business and legal communities, privacy advocates, the general public, and the media regarding the implementation and enforcement of this bill. The OAG indicates that additional resources would be needed to undertake enforcement efforts and would require additional resources for receiving and processing privacy rights complaints and for the investigation and litigation of cases including the retention of consulting experts. Enforcement would require analyzing complaints; identifying issues and alleged violations of the law; issuing civil investigative demands; reviewing and evaluating data protection assessments; conducting factual and legal research to assess violations and viability of potential claims and defenses; retaining and conferring with consulting experts; and litigation activities including discovery, motions practice, preparing for trial, trial, and appeal.

OAG staff would need to devote time to provide feedback to DIR as it prepares a legislatively mandated report regarding the implementation of this bill and recommendations regarding the changes to the law.

The OAG indicates that they would need twelve additional FTEs to handle the anticipated increase in workload resulting from this bill. These additional FTEs include two Assistant Attorney General (AAG) II, two AAG IV, one AAG VI, one Compliance Analyst II, one Data Analyst II, one Data Analyst V, one Legal Assistant I, one Legal Assistant III, one Programmer VI, and one System Administrator V to handle the increased workload. The FTE costs are \$1,520,760 in fiscal year 2024 and \$1,460,370 each fiscal year thereafter. Costs include salary, general operating, travel, capital equipment (technology related and furniture), and benefits.

The Office of Court Administration, Commission on Judicial Conduct, Comptroller of Public Accounts, Department of Information Resources, Bond Review Board, Texas Medical Board, Health & Human Services Commission, Department of Transportation, Texas A&M University System, UT University System, Higher Education Coordinating Board, and Alamo Community College all anticipate no significant fiscal impact from the provisions of the bill. The Comptroller of Public Accounts indicates that the amounts and timing of any penalty revenue are unknown, but is unlikely to be significant.

#### **Technology**

The technology impact includes one-time costs of \$3,563,850 in fiscal year 2024 for the creation of the system, project management costs of \$250,000 each year in fiscal years 2024 and 2025, and a recurring cost in each fiscal year of \$245,606. One-time costs include system development, project management costs, standard laptop, software, printer, and telecom/voicemail. Annual recurring charges cover consulting costs for technology experts, data center services, and voice line.

# **Local Government Impact**

No significant fiscal implication to units of local government is anticipated.

Source Agencies: 212 Office of Court Administration, Texas Judicial Council, 242 State Commission on Judicial Conduct, 302 Office of the Attorney General, 304 Comptroller of Public Accounts, 313 Department of Information Resources, 352 Bond Review Board, 503 Texas Medical Board, 529 Health and Human Services Commission, 601 Department of Transportation, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration, 781 Higher

**Education Coordinating Board** 

LBB Staff: JMc, SZ, LCO, HGR

## FISCAL NOTE, 88TH LEGISLATIVE REGULAR SESSION

# March 12, 2023

TO: Honorable Oscar Longoria, Chair, House Committee on Business & Industry

FROM: Jerry McGinty, Director, Legislative Budget Board

IN RE: HB4 by Capriglione (Relating to the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities; imposing a civil penalty.), As Introduced

Estimated Two-year Net Impact to General Revenue Related Funds for HB4, As Introduced: a negative impact of (\$7,536,192) through the biennium ending August 31, 2025.

The bill would make no appropriation but could provide the legal basis for an appropriation of funds to implement the provisions of the bill.

## General Revenue-Related Funds, Five- Year Impact:

Fiscal Year	Probable Net Positive/(Negative) Impact to General Revenue Related Funds
2024	(\$5,580,216)
2025	(\$1,955,976)
2026	(\$1,705,976)
2027	(\$1,705,976)
2028	(\$1,705,976)

Fiscal Year	Probable Savings/(Cost) from General Revenue Fund 1	Change in Number of State Employees from FY 2023
2024	(\$5,580,216)	12.0
2025	(\$1,955,976)	12.0
2026	(\$1,705,976)	12.0
2027	(\$1,705,976)	12.0
2028	(\$1,705,976)	12.0

The bill amends the Business & Commerce Code by adding Chapter 541, The Texas Data Privacy and Security Act (TDPSA), to address the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities. TDPSA provides consumers residing in Texas with certain rights regarding personal data. These include: the right to request confirmation of whether a controller is processing the consumer's personal data; the right to correct inaccuracies in personal data; the right to delete personal data provided by or obtained about the consumer; the right to obtain data (if feasible) in a portable, readily usable format so that the consumer may transmit it to another controller; and the right to opt out of the processing of personal data for purposes of targeted advertising, sale of personal data, or profiling "in furtherance of a decision that produces a legal or similarly significant effect."

TDPSA requires that controllers provide consumers with notice when they decline to act regarding a consumer's request and to provide justification for declining to act and additionally, to provide instructions on how to appeal the decision. Controllers must provide information in response to a consumer request free of charge, up to twice annually per consumer - unless the request is unfounded, excessive, or repetitive, in which case the consumer may be charged a reasonable fee to cover administrative costs. Controllers must establish a process for consumers to appeal their decisions. If the controller denies an appeal, the controller must provide the consumer with an online mechanism, if available, or another method to contact the OAG to submit a complaint.

The bill requires that certain specific provisions be included in contracts between controllers and processors. The Office of the Attorney General (OAG) has exclusive authority to enforce the provisions of this bill and may obtain injunctive relief, civil penalties of up to \$7,500 per violation, and reasonable attorneys' fees and investigative expenses. Penalties recovered are to be deposited in the general revenue fund.

If the OAG has "reasonable cause to believe" that a person has engaged in, is engaging in, or is about to engage in a violation of this bill, the OAG may issue a civil investigative demand (CID). The bill specifically authorizes the OAG to issue CIDs to controllers requesting relevant data protection assessments and requires controllers to provide those to the OAG. These assessments are confidential and exempt from the Texas Public Information Act, and disclosure to the OAG is not waiver of attorney client or work product privilege regarding information in the assessment. The procedure for CIDs are those established under Texas Business & Commerce Code section 15.10.

Before bringing an action, the OAG is required to provide written notice of specific violations. If the person cures the identified violation within 30 days and provides a written statement that the violations have been cured and that no further violations will occur, the OAG may not bring an action. Violations of the bill following the 30-day cure period and breaches of the written statement provided to the OAG are subject to enforcement actions including a civil penalty of up to \$7,500 per violation.

#### Methodology

The OAG estimates that enactment of the bill will generate an increased number of inquiries from lawmakers, business and legal communities, privacy advocates, the general public, and the media regarding the implementation and enforcement of this bill. The OAG indicates that additional resources would be needed to undertake enforcement efforts and would require additional resources for receiving and processing privacy rights complaints and for the investigation and litigation of cases including the retention of consulting experts. Enforcement would require analyzing complaints; identifying issues and alleged violations of the law; issuing civil investigative demands; reviewing and evaluating data protection assessments; conducting factual and legal research to assess violations and viability of potential claims and defenses; retaining and conferring with consulting experts; and litigation activities including discovery, motions practice, preparing for trial, trial, and appeal.

OAG staff would need to devote time to provide feedback to DIR as it prepares a legislatively mandated report regarding the implementation of this bill and recommendations regarding the changes to the law.

The OAG indicates that they would need twelve additional FTEs to handle the anticipated increase in workload resulting from this bill. These additional FTEs include two Assistant Attorney General (AAG) II, two AAG IV,

one AAG VI, one Compliance Analyst II, one Data Analyst II, one Data Analyst V, one Legal Assistant I, one Legal Assistant III, one Programmer VI, and one System Administrator V to handle the increased workload. The FTE costs are \$1,520,760 in fiscal year 2024 and \$1,460,370 each fiscal year thereafter. Costs include salary, general operating, travel, capital equipment (technology related and furniture), and benefits.

The Office of Court Administration, Commission on Judicial Conduct, Comptroller of Public Accounts, Department of Information Resources, Bond Review Board, Texas Medical Board, Health & Human Services Commission, Department of Transportation, Texas A&M University System, UT University System, Higher Education Coordinating Board, and Alamo Community College all anticipate no significant fiscal impact from the provisions of the bill. The Comptroller of Public Accounts indicates that the amounts and timing of any penalty revenue are unknown, but is unlikely to be significant.

#### **Technology**

The OAG would need to create a new Consumer Data Privacy System supporting consumers from the initial complaint through investigation, litigation, collection of payment, and case closure. The new system would be delivered over a 12-month period using technology industry standard Agile methodologies.

The technology impact includes one-time costs of \$3,563,850 in fiscal year 2024 for the creation of the system, project management costs of \$250,000 each year in fiscal years 2024 and 2025, and a recurring cost in each fiscal year of \$245,606. One-time costs include system development, project management costs, standard laptop, software, printer, and telecom/voicemail. Annual recurring charges cover consulting costs for technology experts, data center services, and voice line.

# **Local Government Impact**

No significant fiscal implication to units of local government is anticipated.

Source Agencies: 212 Office of Court Administration, Texas Judicial Council, 242 State Commission on Judicial Conduct, 302 Office of the Attorney General, 304 Comptroller of Public Accounts, 313 Department of Information Resources, 352 Bond Review Board, 503 Texas Medical Board, 529 Health and Human Services Commission, 601 Department of Transportation, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration, 781 Higher Education Coordinating Board

LBB Staff: JMc, SZ, LCO, HGR