Jurisdiction	Texas
Date	4/20/22
Law Firm	Polsinelli (https://www.polsinelli.com/)
Title, Name	Elizabeth (Liz) Harding, Shareholder Allison Krause, Associate
Contact Information	eharding@polsinelli.com, akrause@polsinelli.com

Questionnaire

I. Law concerning protection of personal information

i. Does your state have a general law concerning the protection of personal information in the private sector at the present or in the near future? No.

ii. Does your state have a general law concerning protection of personal information in the public sector at the present or in the near future? No.

iii. Does your state have laws concerning protection of personal information which apply in individual (specific) sectors at the present or in the near future? (If yes, please describe outline.) No.

*There is no comprehensive law regarding the protection of personal information in Texas. However, in 2007, Texas enacted a data breach notification law, Tex. Bus. & Com. Code §§ 521.002, 521.053, as amended (the "**TDBA**"). The TDBA is similar to many other U.S. state laws regarding notification of data security breaches. In addition, while state agencies are not subject to TDBA directly, Tex. Govt. Code § 2054.1125 ("**TGDBA**") applies to all state agencies in Texas, and incorporates the requirements under the TDBA. Unless stated otherwise in this report, all references to the TDBA, include the TDBDA.*

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I..(please add a reply column as necessary,)

The title of the law ：*Tex. Bus. & Com. Code*

URL:
https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm#521.002

Enforcement status: *Enacted on April 1, 2009, amended on September 1, 2012, June 14, 2013, January 1, 2020, September 1, 2021*

The title of the law: *Security Breach Notification by State Agency*
URL:
https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm#2054.1125
Enforcement status: *Enacted on September 1, 2009, amended on September 1, 2017, September 1, 2019*

① The definition of "Personal Information"	*1. Personal identifying information means information that alone or in conjunction with other information identifies an individual, including an individual's:* *A. Name, social security number, date of birth, or government-issued identification number;* *B. Mother's maiden name;* *C. Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;* *D. Unique electronic identification number, address, or routing code; and* *E. Telecommunication access device as defined by Section 32.51, Penal Code.* *2. Sensitive personal information ("**SPI**") includes an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:* *A. Social Security Number* *B. Driver's license number or government-issued ID number; or* *C. Account number or credit card number or debit card number in combination*

	with any required security code, access code or password that would permit access to an individual's financial account. *SPI also includes information that identifies an individual and relates to:* *D. The Physical or mental health or condition of the individual;* *E. The provision of health care to the individual; or* *F. Payment for the provision of health care to the individual.* *It should be noted that "SPI" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.*
② The scope in which the law applies	*The TDBA applies to all private entities that conduct business in Texas and owns or licenses computerized data that includes sensitive personal information; provided however, financial institutions are not subject to the TDBA.*
③ The territorial scope	*The TDBA applies to data subjects located in Texas, but also businesses operating outside of Texas must also comply with the law.*

ii. If there are any special instructions about the laws, please describe them.

***[Identity Theft**. A person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent or effective consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.]*

***Protection of Personal Data**. A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any SPI collected or maintained by*

the business.

A business shall destroy or arrange for the destruction of customer records containing SPI within the business's custody or control that are not to be retained by the business by:

(1) shredding;
(2) erasing; or
(3) otherwise modifying the SPI in the records to make the information unreadable or indecipherable through any means.

Notification Obligations. *In the event of a data breach of SPI, businesses and state agencies must notify affected individuals. In addition, a business or state agency that is required to provide notification of a security breach of at least 250 Texas residents, must also notify the Attorney General of that breach within 60 days. As of September 1, 2021, the Attorney General will publish a list of notification it receives from businesses under the TDBA for a period of one year, unless such entity experiences another data breach.*

In addition, under the TGDBA, within 48 hours after the discovery of a breach, suspected breach or unauthorized exposure of SPI, state agencies must notify: (a) its department, including its chief information security officer or, (b) the secretary of state if the breach, suspected breach or unauthorized exposure involves election data.

In addition, under the TGDBA within 10 days after the date of eradication, closure and recovery from a breach of SPI, a state agency must notify its department, including the chief information security officer or the details of the event, and include in the notification an analysis of the cause of the event.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your state, please describe the outlines. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

The relevant provision is inapplicable.

(b) Data Quality Principle

While there is no provision specifying this principle, if an entity or public agency experiences an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of SPI, such entity is required to notify the affected individuals, and if applicable the attorney general in Texas.

(c) Purpose Specification Principle

The relevant provision is inapplicable.

(d) Use Limitation Principle

The relevant provision is inapplicable.

(e) Security Safeguards Principle

While there is no provision specifying this principle, if an entity or public agency experiences an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of SPI, such entity is required to notify the affected individuals, and if applicable the attorney general in Texas.

(f) Openness Principle

The relevant provision is inapplicable.

(g) Individual Participation Principle

There is no private right of action under the TDBA, but a violation under the TDBA may also be a violation of the Texas Deceptive Trade Practices Act, which could give rise to a private cause of action.

(h) Accountability Principle

Civil penalties may be brought by the Attorney General in Texas for any violations of at least $2,000 but not more than $50,000 for each violation. In addition, civil penalties for failure to comply with

notification requirements are raised to up to $100 per person to whom notification is due, per day, not to exceed $250,000 per breach.

Also, the Attorney General will publish information related to data breaches of more than 250 Texas residents on a public website for a period of one year.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

IV. Data Localization and Government Access

*While there is no rule regarding Data Localization and Government Access under the laws of Texas, US companies may theoretically be subject to US government surveillance laws, such as Section 702 of the Foreign Intelligence Surveillance Act ("**FISA 702**"), and National Security Letter requests issued by the FBI under Executive Order 12333 ("**EO 12333**" and together with FISA 702, "**US Government Surveillance Laws**"). US government commitments and policies restrict intelligence collection to what is required for foreign intelligence purposes and expressly prohibit the collection of information for other purposes, including commercial advantage.*

*If violations of FISA 702 have occurred, individuals, including Japanese citizens and residents, may seek redress for said violations under several US statutes. An individual who has been subject to unlawful surveillance under FISA may seek damages, punitive damages, and attorney's fees against the individual who committed the violation. In addition, there is a separate private right of action provision under the Electronic Communications Privacy Act ("**ECPA**") for compensatory damages and attorney's fees against the government for FISA Section 702 violations. Further, individuals may also challenge unlawful FISA surveillance through the Administrative Procedures Act, 5 U.S.C. § 702 (2018), which allows individuals "suffering legal wrong because of" certain government conduct to seek a court order enjoining that conduct. Thus, as described above, Japanese citizens or residents, may seek redress for violations of FISA Section 702.*

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

None.