Articles + Publications | May 31, 2023

Locke Lord QuickStudy: Texas Data Privacy and Security Act

Locke Lord LLP

WRITTEN BY

Laura L. Ferguson | Caitríona Pagni

RELATED OFFICES

Houston

After passing the Texas Senate on May 10, 2023, the Texas Data Privacy and Security Act (the "TDPSA")[1] was reconciled by the conference committee between the Texas Senate and House and awaits final approval from Governor Greg Abbott.[2] The TDPSA is intended to be a comprehensive regime for how consumers and companies interact with personal data, maximizing "both the utility of the rights provided to consumers and interoperability with other states to minimize compliance costs for businesses."[3] However, as we have seen with many other state consumer privacy statutes to date, the law is not consistent and defines terms in a different manner than other state comprehensive privacy regimes.

- **Compliance Date and Enforcement Authority**: If signed by Governor Abbott, the majority of the TDPSA will go into effect on July 1, 2024 with a delayed effective date of January 1, 2025 with respect to the ability for consumers to designate an authorized agent to act on their behalf for a request to opt out of processing. The TDPSA grants exclusive enforcement and investigative authority to the Texas Attorney General. The TDPSA directs the Texas Attorney General to provide consumers: (1) information outlining consumer rights and the responsibilities of controllers[4] and processors under the TDPSA and (2) an online portal for submitting consumer complaints by July 1, 2024.

The Texas Attorney General must notify an individual or entity of an alleged violation of the TDPSA at least 30 days before bringing an enforcement action. Upon receiving notice, the person has a 30-day cure period to resolve the violation and provide a written statement attesting that the privacy violation was cured, the consumer was notified that the privacy violation was addressed (if contact information was available), documentation to show the violation was cured, and changes to internal policies as necessary to prevent future violations.

If a violation is not cured within 30 days or the written statement to the Texas Attorney General is violated, the offending individual or entity may face penalties including: civil penalties of up to $7,500 for each ?violation? and/or injunctive relief to restrain or enjoin the person's operations. Additionally, the person will be liable for reasonable attorney's fees and other expenses incurred from investigating and bringing an action under the TDPSA.

The TDPSA does not provide a private right of action.

- **Who is subject to the TDPSA?** The TDPSA applies broadly to individuals and entities that process or engage in the sale of personal data and (1) conduct business in Texas or (2) produce a product or service consumed by residents of Texas. Therefore, businesses can be covered in Texas even if they neither do business in Texas

nor target marketing to Texas residents. Unlike other state consumer privacy laws that exempt businesses from their privacy regimes based on revenue or data volume thresholds, the TDPSA casts a wider net by exempting "small businesses" as defined by the U.S. Small Business Administration, except to the extent that the small business engages in the sale of sensitive personal data (discussed further below).[5] Also exempt are financial ?institutions subject to Title V of the Gramm-Leach-?Bliley ?Act; HIPAA covered entities and businesses ?associates; and state agencies and political subdivisions, certain nonprofit organizations[6], higher ?education institutions, and electric utilities, power generation companies, or retail electric providers[7].

- Compliance Note: An individual or entity is conducting business in Texas if the organization maintains intentional, long-term activities in the state including, but not limited to, developing property in Texas, authorizing a franchisee, or maintaining a general purpose office and employees in Texas.[8]
- A small business may not engage in the sale of sensitive personal data without receiving prior consent from the consumer. A violation of this provision is subject to the penalties described above.

- **What consumer rights exist under the TDPSA**? Much like prior legislation such as California's CCPA or Virginia's VCPA,[9] the TDPSA establishes basic consumer rights over personal data, including the right to (1) confirm whether a controller is processing the consumer's personal data; (2) opt out of data processing for targeted advertising, sales of personal data, or profiling to inform certain decisions that will affect the consumer; (3) and access, correct, delete, and obtain a copy of the consumer's data. Additionally, any provision of a contract or agreement may not waive or limit these consumer rights.
  - Compliance Note: the TDPSA defines "consumer" as an individual who is a resident of Texas **acting only in an ?individual or household context**. The term does not include an ?individual acting in a commercial or employment context. ?
- **What data is exempt from the TDPSA**? The TDPSA creates carve outs for the following categories of data: (1) health records, patient identifying information, and other protected health information under HIPAA; (2) health records; (3) identifiable private information for purposes of the federal policy for the protection of human research ?subjects; (4) information and documents created for purposes of the Health Care ?Quality Improvement Act?; (5) patient safety work product collected for purposes of the Patient Safety and ?Quality Improvement Act; (6) information derived from health care-related information that is de-identified in accordance with HIPAA; (7) information originating from, and intermingled to be indistinguishable with, or treated in the same manner as, information exempt maintained by a HIPAA covered entity or business associate; (8) information included in a limited data set as described in HIPAA (if used in compliance with HIPAA); (9) information collected or used for public health activities as permitted by HIPAA; (10) personal information collected in furtherance of activities that are regulated by and authorized under the Fair ?Credit Reporting Act; (11) personal data collected, processed, sold, or disclosed in ?compliance with the Driver's Privacy Protection Act; (12) ?personal data regulated by the Family Educational Rights and ?Privacy Act?; (13) personal data collected, processed, sold, or disclosed in ?compliance with the Farm Credit Act?; (14) data processed or maintained in the course of an individual applying ?to, employed by, or acting as an agent or independent contractor of ?a controller, processor, or third party, ?if that data is collected and used within the context of that role?; (15) data processed or maintained as emergency contact information; (16) data processed or maintained and necessary to retain to administer benefits for another individual that relates to an employee/agent/independent contractor of a controller, processor, or third party; and (17) data subject to Title V, Gramm-Leach-?Bliley ?Act[10].
- **What's different from other state comprehensive privacy laws**? The TDPSA is intended to build on standards promulgated by the VCPA to heighten accountability for businesses that utilize consumer data, clarify ambiguities that arose under the VCPA, and enhance "best practices" for businesses regarding data processing, sharing, and protection. Here are some of the key provisions to note:
  - ***Definition of Personal Data***: the TDPSA distinguishes between "de-identified data" (which cannot be attributed to an individual) and "pseudonymous data" (which cannot be attributed to an individual without additional information). The statute includes "pseudonymous data" under its definition of "personal data" only when used by a controller or a processor in conjunction with additional information that reasonably links the data to an identified or an identifiable individual. Additionally, the statute establishes handling requirements for both types of data to prevent re-identification.
  - ***Definition of Consent***: the TDPSA narrows its definition of consent to exclude (1) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (2) hovering over, muting, pausing or closing a given piece of content; or (3)

agreement obtained through the use of dark patterns.[11] This narrowed definition of consent is designed to deter businesses from steering consumers toward conceding personal information by obscuring key privacy policy information by nesting it in other unrelated information.

- ***Definition of "Sale" of Personal Data***: The TDPSA adopts a broader definition of "sale" of data to encompass "sharing, disclosing, or transferring of personal data." The definition also expands the types of transactions that would qualify as a sale of data to include both monetary transactions and quid pro quo agreements.
- ***Consumer Requests***: The TDPSA merges the VCPA and the CCPA's mandated procedures for making consumer requests by requiring covered businesses to provide two secure and accessible means for consumers to submit requests for data. The TDPSA also clarifies the consumer's right to access their data to ensure all digitally available information may be accessed by the consumer, regardless of the method a business uses to process the consumer's data.
- ***Privacy Notice Disclosure of Collection of Sensitive Data (including Biometric Data)***: The TDPSA requires businesses to disclose any collection of sensitive data, which includes biometric data (data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retina or iris, or other unique biological patterns or characteristics), in their privacy policies.

- ***Exemptions for Information Collected for Public Health Activities and Trade Secrets*:** The TDPSA expands its exemption for public health activities conducted by agencies such as the FDA to include "information collected or used only for public health activities." This exemption confirms that FDA-regulated entities may comply with federal requirements when handling public health data. The statutes also defines "trade secrets" to align with the definition set forth in the Texas Uniform Trade Secrets Protection Act[12] and creates an exemption for such information from the requirements of the act.

Recommended Compliance Steps

Individuals and entities subject to the TDPSA, should take the following measures to ensure compliance:

- *Data Protection Assessment.* Conduct a data protection assessment of the types of data[13] your organization collects and evaluate how that data is used across your organization to determine if the data qualifies as "personal data" as defined by the TDPSA. The assessment must identify and weigh the direct or indirect benefits that the organization may gain from use of personal data against the potential risks to the ?rights of the consumer associated with that processing, as ?mitigated by safeguards that can be employed to ?reduce the risks. The assessment must also consider: the use of de-identified data; ? the reasonable expectations of consumers; ? the context of the processing; and the relationship between the controller and the ?consumer whose personal data will be processed.? The results of this assessment must be made available to the Texas Attorney General.
- *Limit and Protect Personal Data.* Ensure your organization both (1) limits the collection of personal data to what is adequate, ?relevant, and reasonably necessary in relation to the purposes for ?which that personal data is processed, as disclosed to the ?consumer; and (2) utilizes reasonable administrative, technical, and ?physical data security practices that are appropriate to the volume ?and nature of the personal data your organization handles.?
- *Establish and Assess Disclosure and Consent Requirements.* Evaluate your organization's processes for obtaining consent to collect, utilize and share data to ensure they comply with the TDPSA's requirements for consent. Revise/draft privacy policies to comply with the TDPSA's consent definition, avoiding ?obscuring privacy disclosures with other generalized information, hover-over content or other ?UI/UX designs that could obscure information, and other "dark patterns" that could otherwise ?impair consumers' understanding of your privacy practices. ?
- *Revise or Draft a Consumer-facing Privacy Notice.* The privacy notice must describe any processing of personal data, including any biometric and other sensitive data, the purposes for processing personal data, and articulate

the TDPSA's consumer rights and methods to submit requests, describes categories of personal data shared with third parties and the categories of third parties who receive such data. If the controller sells sensitive personal data, a specific disclosure must be included.[14] For businesses subject to other state privacy laws, existing notices may be able to be leveraged.

- *Organize for Receiving and Processing Consumer Requests.* Assess and update IT governance practices to ensure your organization offers adequate and accessible means for consumers to submit requests for data. Most organizations must provide at least two secure and reliable methods to enable consumers to ?submit a request to exercise their consumer rights?, and these methods must consider: (1) the ways in which consumers normally interact with the controller; (2) the necessity for secure and reliable communications of those requests; and (3) the ability of the controller to authenticate the identity of the consumer making the request. Additionally, if your organization operates a website, you must make the website available to consumers to submit requests for ?information?. If your organization operates exclusively online and has a collects personal information directly from consumers, then you are ?only required to provide an e-mail address for the submission of ?requests. ?
- *Establish Response Protocols for Response to Consumer Requests.* Update or adopt procedures to ensure your organization can respond to consumer requests for data within 45 days of receipt of the ?request. The controller may extend the response period once by an ?additional 45 days when reasonably necessary, but ?the controller must inform the consumer of the extension? within the initial 45 day period.
- *Confirm Retention and Deletion Process.* Assess IT governance practices to ensure your organization meets the TDPSA's requirements to adequately delete consumer information as necessary.
- *Assess, Manage and Disclose "Sales."* Review contracts with third parties that involve the "sale" of personal information as defined under the TDPSA to ensure all sales meet the statute's requirements. If your organization sells personal data to third parties or processes ?personal data for targeted advertising, you must clearly and conspicuously disclose such processing and the manner ?in which a consumer may exercise the right to opt out of such ?processing?.

—

[1] Full text of the TDPSA

[2] As of the date of publication, the TDPSA is awaiting final signature by the governor.

[3] Committee Report, C.S.H.B. 4

[4] The TSPSA defines "controller" as include "an individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data." H.B. 4 Sec.? 541.001(8)

[5] The Office of Advocacy defines a small business as an independent business having fewer than 500 employees.

[6] The TDPSA exempts: (i) nonprofits organized under Chapters 20 and 22, Texas Business Organizations Code, and the provisions of Title 1, Texas Business Organizations Code; (ii) 501(c)(3), 501(c)(6), 501(c)(12) and 501(c)(19) entities; (iii) 501(c)(4) entity that is also described by Section 701.052(a) of the Texas Insurance Code; and (iv) political organizations.

[7] See Section 31.002, Utilities Code, for definitions of an electric utility, a power generation company, or a retail electric provider.

[8] Texas law defines “transacting business” in the negative, stipulating that transacting business does not include: 1) maintaining, defending, or settling any proceeding; 2) holding meetings of officials or members or carrying on the internal affairs of the entity; 3) maintaining bank accounts; 4) maintaining an office or agency for the transfer, exchange, or registration of interests of the entity; 5) voting the interest of an entity the foreign entity has acquired; 6) making sales through independent contractors; 7) creating, as borrower or lender, or acquiring an indebtedness or security interest in real or personal property; 8) securing or collecting debts; 9) transacting business in interstate commerce; 10) conducting an isolated transaction; 11) exercising a power of executor of a will of a non-resident, as administrator of a will of a non-resident decedent, or as trustee of a trust created by non-residents or foreign entity; 12) acquiring a debt on property inside the state by a transaction outside of the state; 13) investing or acquiring a royalty or non-operating mineral interest in a transaction outside of the state; 14) executing a division order, contract of sale, or other instrument incidental to ownership of a non-operational mineral interest; 15) owing, without more, property in the state; or 16) acting as a governing person of a domestic or foreign entity registered to transact business in the state. Tex. Business Organizations Code § 9.251

[9] Comparison of a prior version of the TDPSA and VCPA.

[10] While Section 541.003 describing information exempt from the TDPSA does not mention data subject to the Title V, Gramm-Leach-?Bliley ?Act (“GLBA”), the exemptions under Section 541.002(b) describing entities not subject to the TDPSA includes a reference to “or data” under (b)(2) with respect to the GLBA.

[11] “Dark pattern” means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is not limited to, any practice the Federal Trade Commission refers to as a “dark pattern”. H.B. 4 Sec. 541.002 (10).

[12] “Trade secret” means all forms and types of information, including business, scientific, technical, economic, or engineering information, and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: (A) the owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information H.B. 4 Sec. 541.002 (33).

[13] Types of data that must be assessed are: ?(1) the processing of personal data for purposes of targeted ?advertising;? ?(2) the sale of personal data;? (3) the processing of personal data for purposes of ?profiling, if the profiling presents a reasonably foreseeable risk ?of:? (A) unfair or deceptive treatment of or unlawful ?disparate impact on consumers;? (B) financial, physical, or reputational injury to ?consumers;? (C) a physical or other intrusion on the solitude ?or seclusion, or the private affairs or concerns, of consumers, if ?the intrusion would be offensive to a reasonable person; or (D) other substantial injury to consumers;? ?(4) the processing of sensitive data; and (5) any processing activities involving personal data ?that present a heightened risk of harm to consumers.?

[14] As applicable to the data, the notice should include one or both of the following: (i) “NOTICE: We may sell

your sensitive personal data."; and (ii) "NOTICE: We may sell your biometric personal data."

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber