KANE RUSSELL COLEMAN LOGAN

Eight Steps Businesses Can Take to Comply with the Texas Data Privacy and Security Act in Advance of the July 1, 2024 Effective Date

Jamie Wilson

The Texas Data Privacy and Security Act ("TDPSA") regulates the collection, use, processing, and treatment of consumers' personal data. The TDPSA applies to nearly anyone who conducts business in Texas or produces products or services consumed by Texans and who processes or engages in the sale of personal data. The TDPSA imposes obligations on businesses to restrict the type of personal data that can be collected, obtain consent for collection of certain "sensitive" data, provide notices regarding the data that is collected, and conduct "data protection assessments."

Because the majority of the TDPSA's provisions will take effect on **July 1, 2024**, it is imperative for businesses operating in Texas or providing products or services to consumers within the State of Texas to determine: (1) whether they must comply with the TDPSA; and (2) how to comply before its effective date.

What is the TDPSA?

The TDPSA provides Texas residents with certain rights with respect to their personal data, including rights of access, correction, deletion, and portability. It also includes the right to opt out of the processing, sale, or profiling of their personal data for the purposes of targeted advertising and the right to appeal a business's decision regarding a rights request. The TDPSA only protects consumers acting in an individual or household capacity, meaning it is not applicable in business-to-business (B2B) contexts.

The TDPSA defines "personal data" as any information that identifies, relates to, describes, or is capable of being associated with an individual, including but not limited to name, address, email address, social security number, driver's license number, passport number, or any other identifier that permits the physical or online contacting of a specific individual.

The TDPSA provides additional protections for "sensitive data," which includes data on racial or ethnic origin, religious beliefs, health diagnoses, sexuality, citizenship or immigration status, genetic or biometric information, information from a known child, and geolocation data. For businesses to process sensitive data in compliance with the TDPSA, they must also obtain consent from the consumer. When obtaining the consumer's consent, businesses are prohibited from using any interfaces that encourage the consumer to provide the most personal information.

Who must comply with the TDPSA?

The TDPSA applies to individuals and entities who conduct business in Texas or produce a product or service consumed by Texas residents and process or engage in the sale of personal data.

Under the TDPSA, businesses are classified into "controllers" and "processors." "Controllers" are those who determine the purpose and means of processing personal data. Examples of controllers include retailers, merchants, restaurants, heath care providers, as well as law firms. "Processors" are entities who process personal data on behalf of the controller. Examples of processors include payroll companies, third-party marketing companies, data analytics companies, software providers, and cloud service providers. In some circumstances, a business can be both a controller and a processor. For example, when a business processes payroll for its own employees, it is both a controller with regards to the data it collects on its employees and a processor with regards to the data processed for payroll.

The TDPSA imposes specific obligations on controllers to limit the collection of personal data to what is relevant and reasonably necessary in relation to the purpose for which the data is collected. Processors must abide by the controller's instructions in regards to processing the personal data and assist the controller in complying with the TDPSA's requirements. The TDPSA also provides requirements that must be included in the contracts between controllers and processors.

Controllers are also required to provide a privacy notice or policy disclosing the data that the controller collects, the purpose for which it collects the data, the consumer's rights regarding the collected data, and how to exercise those rights.

Additionally, controllers are obligated to conduct mandatory "data protection assessments" if they: (1) process personal data for targeted advertising; (2) take part in the sale of personal data; (3) process personal data for the purposes of profiling; (4) process sensitive data; or (5) engage in any processing activities involving data that present an increased risk of harm to consumers.

Who is exempt from the TDPSA?

Numerous entities are exempt from complying with the TDPSA. Some of these include state agencies and political subdivisions of Texas, financial institutions subject to Title V of the Gramm-Leach-Bliley Act, entities or business associates governed by HIPAA, non-profit companies, institutions of higher education, electric utility and power generating companies, retail electric providers, and small businesses that do not sell sensitive personal data.

What are the penalties for violations of the TDPSA?

Before imposing penalties for violations of the TDPSA, the Texas Attorney General's office must provide notice of the violation and a 30-day period to cure such violation. If a violation is not cured within 30 days, 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 offending operations. Notably, consumers do not have a private right of action for TDPSA violations.

What steps can businesses take now to comply with the TDPSA?

Businesses can comply with the TDPSA by taking the following steps:

1. Generating or updating website privacy notices to include the specific disclosures required by the TDPSA. If your business is a controller, the privacy notice must include: (1) the categories of personal data to be processed including any sensitive data; (2) the purpose of processing; (3) how consumers may exercise their rights and appeal refusals; (4) the categories of data shared with third parties; (5) the categories of third parties with whom the controller shares data; and (6) at least two methods for consumers to submit requests. If your business sells sensitive data, the privacy notice must also include the following disclosure: "NOTICE: We may sell your sensitive personal data," or biometric data: "NOTICE: We may sell your biometric personal data."

2. Implementing reasonable security measures to prevent unauthorized access, use, or disclosure of personal data. This includes encryption, firewalls, authentication protocols, regular risk assessments, and access controls that limit data access only to authorized individuals within the organization who have a legitimate need for such access. Businesses should also establish incident response plans to address potential data breaches or security incidents. This includes procedures to promptly notify affected individuals and, in certain cases, regulatory authorities in the event of a data breach.
3. Obtaining consent from consumers if you collect sensitive data. You can do this by generating or updating your cookie policy and including opt-out options on consent banners.
4. Implementing a process for consumers to exercise their rights under the TDPSA, such as the right to access, delete, or correct their personal data. One method is to implement a Data Subject Access Request (DSAR or SAR) form on your website or platform and link to it in your privacy policy. It is also essential to establish protocols for responding to consumer requests.
5. Reviewing and updating contracts with vendors who process personal data to ensure compliance with the TDPSA. The contract should include instructions for data processing, the purpose and nature of processing, the type of data being processed, the duration of processing, the rights and obligations of both parties, confidentiality and data protection obligations, data deletion or return after service completion, availability of information for compliance demonstration, cooperation with assessments, and engagement of subcontractors under similar contractual terms.
6. Conducting data protection assessments, if required. This includes identifying and weighing the potential direct or indirect benefits to the controller, the consumer, other stakeholders, and the public from processing the personal data against any potential risks to the consumer's rights.
7. Conducting regular risk assessments to identify vulnerabilities and potential threats to consumers from the collection of personal data. This allows businesses to proactively implement measures to mitigate vulnerabilities and enhance their overall data security to comply with the TDPSA.
8. Training and educating employees and staff about data privacy and security best practices. By doing this, businesses can minimize the risk of data breaches and ensure overall compliance with the TDPSA.

Businesses that operate in Texas or conduct business with Texas residents should immediately begin implementing processes to comply with the TDPSA. Taking action now not only potentially avoids potential penalties, but it demonstrates a commitment to protecting consumer data. Doing so can also enhance consumer perception and trust of the company and differentiate itself from its peers.

About the Author

Jamie R. Wilson is a dedicated litigator committed to achieving proven, cost-effective results tailored to the needs of his clients. Jamie's practice focuses on complex commercial litigation involving employment and contractual disputes and other matters involving businesses. He has extensive experience handling cases involving trade secrets as well as non-competition agreements, non-solicitation agreements, and other restrictive covenants.

If you have any questions or would like to discuss the topic, Jamie is available via email at: jwilson@krcl.com and phone at: 214-777-4285.