Texas Passes Comprehensive Consumer Privacy Bill

July 6, 2023 Gavin George, Tim Newman

PRACTICES Privacy and Cybersecurity

With the Texas governor's recent approval of the Texas Data Privacy and Security Act (the "TDPSA" or the "Act"), Texas becomes the tenth state to enact a comprehensive consumer data privacy statute. The Act was signed by Governor Greg Abbott on June 18, 2023 and will largely take effect July 1, 2024. The Act establishes consumer rights commonly seen in other state privacy laws and requires businesses to implement new processes for handling personal data and consumer inquiries about that data. Businesses subject to the law should begin preparing for the statute's effective date now.

Background

The TDPSA is the most recent comprehensive privacy law to be enacted in 2023.[1]The Act is modeled after the Virginia Consumer Data Protection Act, but has some unique characteristics, including novel approaches to the scope of affected businesses, definitions of key terms, data controller obligations, and opt-in consent requirements for businesses processing sensitive personal data. The Act balances strong consumer rights with some business-friendly provisions and will create a privacy regime unlike that of other states.

Applicability and Exemptions

The Act applies to all persons that: (1) conduct business in Texas or produce goods or services consumed by residents of the State of Texas; (2) process or engage in the sale of personal data; and (3) are not a small business as defined by the U.S. Small Business Administration, unless otherwise exempt from coverage by the statute.[2] State agencies, nonprofits, higher education institutions, financial institutions, electric utilities and providers, and covered entities or business associates subject to the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act are exempt from the Act.

The Act also generally exempts from its coverage certain specific categories of personal data already protected by federal laws or other regulations in the healthcare, financial services, public health, education, and other sectors.

Controller and Processor Obligations

The TDPSA imposes certain familiar obligations on controllers and processors of personal data. Under the Act, a "controller" is defined as "an individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data." "Processing," in turn, is defined as "an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data."

The TDPSA requires controllers to limit the collection of personal data to what is adequate, relevant, and reasonably necessary to achieve the disclosed processing purposes and requires them to maintain reasonable data security practices appropriate to the volume and nature of the

personal data being processed. They must also disclose to consumers and obtain consent for the processing of certain types of personal data.

Any controller that sells personal data to third parties or processes personal data for targeted advertising must clearly and conspicuously disclose this processing to consumers and must give consumers an option to opt out of the sale or processing of their personal data. A controller also must provide a "clear and accessible" privacy notice describing: (1) the categories of personal data to be processed; (2) the purpose of processing the personal data; (3) how consumers may exercise their consumer rights; (4) the categories of personal data the controller shares with third parties; (5) the categories of third parties with whom the controller shares personal data; (6) a description of the methods consumers may use to submit requests; and (7) additional specific notices required if a controller sells sensitive personal or biometric data.

Finally, the TDPSA requires controllers to conduct an internal data protection assessment if they: (1) process personal data for purposes of targeted advertising, (2) sell personal data, (3) process personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of certain specified harm to consumers, (4) process sensitive data; or (5) engage in any processing activities involving personal data that present a heightened risk of harm to consumers. These data protection assessments must include certain specified components, and must be made available to the attorney general of Texas pursuant to a civil investigative demand. The TDPSA, however, explicitly states that the submitted data protection assessments are not subject to public inspection and copying under the Texas Public Information Act.

The TDPSA defines a "processor" as "a person that processes personal data on behalf of a controller." Generally, the TDPSA requires processors to assist controllers in complying with the Act, including assisting controllers in responding to consumer rights requests, ensuring the security of processing personal data, and conducting data protection assessments. The Act also requires controllers and processors to have a contractual relationship that includes certain specified provisions, including provisions aimed at ensuring confidentiality of the data being processed.

Consumer Rights

The TDPSA establishes strong consumer rights, including the right to: (1) understand whether a data controller is processing a consumer's personal data; (2) require correction of inaccuracies in a consumer's personal data; (3) require deletion of personal data; and (4) obtain a copy of a consumer's personal data from a controller. A consumer may also opt-out of the processing of personal data for targeted advertising, sale, or profiling having legal or similarly significant effects regarding the consumer.

Under the Act, controllers will be required to respond to consumer requests to exercise their rights under the Act within 45 days, a deadline which can be extended in certain circumstances. If a controller refuses to take action on a consumer's request, the consumer will have a right to appeal the controller's inaction. Requested information must be provided to consumers free of charge, up to twice annually per consumer.

Enforcement

The TDPSA does not establish a private right of action to enforce consumer rights or other obligations. Instead, the attorney general of Texas will have exclusive authority to enforce the Act. The attorney general's enforcement authority will include the ability to issue civil investigative demands and to bring actions in the name of the State of Texas to recover civil penalties.

Before suit is brought, however, the Act requires the attorney general to notify a person suspected of violating the statute in writing and give the alleged violator a 30-day period to cure the specific alleged violation. Alleged violators must not only cure the violation within that time period, but they must also submit a written statement to the attorney general confirming the alleged violation was cured, notify the relevant consumer, provide supporting documentation to show how the violation was cured, and revise internal policies as needed. Failure to timely cure a violation may result in civil penalties of up to $7,500 for each violation. The attorney general also may pursue injunctive relief, recover reasonable attorney's fees and other expenses incurred in investigating the alleged violation(s), and recover other costs associated with investigating and bringing suit under the Act.

Effective Date and Administrative Timeline

Most provisions of the TDPSA will take effect July 1, 2024. Certain provisions related to the use of authorized agents to exercise consumer rights and requirements related to opt-out preference signals will take effect January 1, 2025.

Amendment to Texas Data Breach Notification Statute

In addition to the TDPSA, Texas Governor Greg Abbott signed SB 768 on May 27, 2023, amending the state's data breach notification statute. Tex. Bus. & Com. Code Ann. § 521.053. The amendment now requires a person who is required to disclose a breach of system security involving at least 250 Texas residents to notify the attorney general "as soon as practicable" and not later than 30 days after the date on which the person determines that the breach occurred. This is a reduction from the prior 60-day deadline. The amendment also requires that notification to be submitted electronically using a form that will be accessible through the attorney general's website. This amendment to the breach notification statute will take effect September 1, 2023.

Conclusion

The TDPSA is a game changer for organizations doing business in Texas or selling products or services to Texas residents and adds to the current patchwork of state privacy laws developing around the country. Creating a compliant privacy program requires a thorough understanding of the categories of personal data an organization collects and stores, how it protects and uses that data, and the relevant legal obligations. Organizations subject to any of these state privacy laws should review their practices and take steps now to avoid any regulatory scrutiny.

[1] The other states that have enacted similar privacy laws in 2023 are Indiana, Iowa, Montana, and Tennessee.

[2] Despite the small business exemption, the Act explicitly requires all covered businesses, regardless of size, to obtain opt-in consent before selling a consumer's sensitive data, defined to include (1) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status; (2) genetic or biometric data that is processed for the purpose of uniquely identifying an individual; (3) personal data collected from a known child; or (4) precise geolocation data.

For more information or assistance complying with the TDPSA or other state privacy laws, contact one of the Haynes Boone lawyers below.