Articles + Publications | April 1, 2024

Texas Joins the State Privacy Law Landscape on July 1, 2024: The Texas Data Privacy and Security Act

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Laura L. Ferguson

RELATED OFFICES

Hartford | Houston

Effective July 1, 2024, Texas will join California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Utah and Virginia, with a new, general consumer privacy statute the Texas Data Privacy and Security Act ("TDPSA"). How is it the same as other state privacy laws, and how is it different? Our comparison chart lines up all of these statutes, as a quick guide for comparative analysis. This article reviews the highlights, including how to determine whether the TDPSA applies to your business, and what is required to come into compliance with the TDPSA.

Applicability. With important exceptions identified below, the TDPSA applies to any person that: (1) conducts business in Texas or produces a product or service consumed by Texas residents; (2) processes or engages in the "sale" of personal data; and (3) is not a small business as defined by the United States Small Business Administration (with the exception that the TDPSA's consent requirement for the sale of sensitive data still applies to an otherwise exempt small business). In contrast to other general consumer privacy laws, which apply to persons "doing business" in the state, the Texas statute extends to persons that produce a product or service consumed by Texas residents, presumably with no other nexus to Texas. This is not necessarily surprising given that the Texas data breach statute requires notification to impacted out-of-state residents if the other state would not otherwise require notice. However, an out-of-state business could potentially challenge the extraterritorial reach of the TDPSA (as well as the breach notification statute) where, for example, a business conducts business online or in other states visited by Texas residents, without any connection to Texas, and without marketing directed to Texas residents.

The TDPSA provides important exemptions for financial institutions and data subject to the federal Gramm-Leach-Bliley Act; HIPAA covered entities and business associates; nonprofits; institutions of higher education; state agencies and political subdivisions; and electric utilities, power generation companies, and retail electric providers. Additional data-based exemptions include employment and human resources data, HIPAA protected health information, data subject to FCRA, and FERPA data. Subject to these and other exemptions, the TDPSA applies to "personal data," defined to mean any information linked or reasonably linkable to an identified or identifiable individual, other than publicly available information.

Consumer Rights. Similar to the other, existing state general consumer privacy statutes, the TDPSA provides consumers with rights to know what personal data is collected, and to access, obtain, delete and correct their

personal data. Consumers will also have the right to opt-out of processing for the purposes of targeted advertising, sales of personal data, and certain profiling.

Persons determining the purpose and means of processing personal data (defined as "controllers") must respond to authenticated consumer requests to exercise their TDPSA rights within 45 days, subject to a "reasonably necessary" extension of up to 45 days. If a controller rejects a consumer request, the controller must inform the consumer within 45 days of the justification, and the consumer's right to appeal. Denials of appeals must include instructions on how to file a complaint with the Attorney General.

Controller Obligations. In addition to the obligations summarized above concerning responses to consumer requests, the TDPSA imposes various obligations on controllers. Collection and processing of personal data must be limited 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." Controllers must also "establish, implement, and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue." The TDPSA prohibits controllers from discriminating against consumers for exercising their rights, and controllers are prohibited from processing sensitive data without the consumer's consent. The TDPSA defines sensitive data to include racial or ethnic origin, religious beliefs, health diagnosis, genetic and biometric data, precise geolocation data, and information about a known child.

Controllers are required to conduct data protection assessments for the processing of personal data for targeted advertising and certain profiling; sales of personal data; processing sensitive data; and processing that presents a heightened risk of harm to consumers. Data protection assessments must balance the benefits to the controller, consumers, other stakeholders and the public against the risks to consumers, mitigated by safeguards. Data protection assessments are exempt from public disclosure and copying requirements of Texas law, but available for inspection by the attorney general.

Notice Obligations. Controllers must provide consumers with a reasonably accessible and clear notice that includes the categories of personal data processed; the purpose for processing; how to exercise consumer rights and appeal decisions by the controller; and the categories of personal data shared with third parties, and the categories of parties with which personal data is shared. Specific disclosures are required if sensitive data or biometric data is sold, and if personal data is sold for targeted advertising. Importantly, the TDPSA provides that a data protection assessment conducted under other statutes and regulations can be used for TDPSA compliance if the assessment has comparable scope and effect.

Processor Obligations. Controllers must enter into contracts with processors that satisfy specific requirements of the TDPSA, and processors are required to follow the controllers' instructions and to assist controllers in satisfying their TDPSA obligations.

Next Steps for Businesses Subject to the TDPSA

- *Conduct data protection assessment*. For businesses already subject to other laws such as Colorado or Connecticut, leveraging the existing DPA will ease this process.
- *Implement or update, as necessary, administrative, technical, and physical data security processes appropriate to the business.*
- *Update privacy program for Texas residents' consumer rights.* For businesses subject to other state laws with

consumer rights, leveraging the existing process should be feasible.

- *Draft a consumer notice.* For businesses subject to other state laws, this should be an exercise of reviewing/confirming the notice is accurate for purposes of Texas residents and the processing of their data.
- *Enter into or update contracts with any processors to include language that satisfies the TDPSA.*

If you would like assistance reviewing and updating your policies and procedures, notices, or otherwise need assistance with compliance with the TPDSA, please contact the authors.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber