



Jun 02, 2023

Categories:

[Publications](#)

[Technology Blog](#)

Authors:

[Michael E. Nitardy](#)

[Jean Paul Yugo](#)

[Nagashima](#)

[Ryan J. Preston](#)

[Lauren E. Cole](#)

Texas Is Next to Pass a Consumer-Friendly, Comprehensive Privacy Law

On May 29, 2023, the Texas legislature passed the Texas Data Privacy and Security Act (TDPSA). The bill must still be signed by the governor by June 9, 2023, in order to become law. If it becomes law, it will go into effect July 1, 2024. Considering that Texas is the second largest state in the U.S., the impact of the bill is likely to be significant. Commentators have already referred to the bill as a “consumer friendly” version of the Virginia privacy bill.

Who Does the TDPSA Apply To?

The TDPSA will apply to companies:

- conducting business in Texas or producing a product or service consumed by residents of the state;
- who process or engage in the sale of personal data; and
- are not otherwise defined as a small business under the U.S. Small Business Administration’s (SBA) definition of a small business.

The SBA has many definitions of a small business depending on the specific industry a company works in, making it an open question as to which specific definition will apply. Generally, a small business is one that has fewer than 500 employees.

Small businesses are still prohibited from engaging in the sale of personal data, specifically sensitive data (defined below), without receiving prior consent from the consumer.

Who Does the TDPSA Protect?

The TDPSA protects “consumers” that are “residents of the state of Texas acting in an individual or household context.” It does not apply to consumers acting in a commercial or employment context.

What Type of Data Is Covered by the TDPSA?

Under the TDPSA, “personal data” is defined as “any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual.” The bill further stipulates, “The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual. The term does not include deidentified data or publicly available information.”

Pseudonymous data is any information that cannot be attributed to a specific individual without the use of additional information if the additional information is kept separately and is protected under appropriate technical and organizational measures.

“Sensitive data” is a category of personal data that is:

- revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status;
- genetic or biometric data that is processed for the purpose of uniquely identifying an individual;
- personal data collected from a known child; or
- precise geolocation data.

Are There Any Prohibitions on How Companies Can Use Personal Data?

Like other state privacy laws, the TDPSA prohibits the “sale of personal data,” defined as “the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the company to a third party. The term does not include:

- The disclosure of personal data to a processor that processes the personal data on the company’s behalf;
- The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
- The disclosure or transfer of personal data to an affiliate of the company;
- The disclosure of information that the consumer: intentionally made available to the general public through a mass media

- channel; and did not restrict to a specific audience; or
- The disclosure or transfer of personal data to a third party as an asset that is part of a merger or acquisition.

What Rights Do Consumers Have Under the TDP SA?

Under the law, consumers have the right to:

- know whether a controller is processing personal data and accessing the personal data;
- correct inaccuracies;
- delete personal data;
- obtain a copy in digital format and transmit to another controller; and
- opt out of
 - targeted advertising,
 - sale of personal data, and
 - profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.

In addition, consumers have a right to appeal a company's response to their requests. Companies must respond to consumer requests within 45 days after receipt of the request (which may be extended by an additional 45 days once if reasonably necessary due to complexity and the number of consumer requests).

Are Privacy Impact Assessments/Data Protection Impact Assessments Needed?

Data protection assessments are required in the event of using personal data in:

- targeted advertising;
- sale of personal data;
- processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of:

- unfair or deceptive treatment of or unlawful disparate impact on consumers,
- financial, physical, or reputational injury,
- 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;
- processing of sensitive data; or
- any processing activities involving personal data that present a heightened risk of harm to consumers.

Who Has Enforcement Authority? And Is There a Private Right of Action?

The Texas attorney general will have exclusive authority to enforce the statute, so there is no private right of action. The attorney general will have an online complaint mechanism available to consumers, and companies that are the target of investigations will have a 30-day right to cure violations of the TDPSA. For more information, please contact the authors or any member of Frost Brown Todd's [Data Security & Privacy](#) practice group.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.