Texas Data Privacy and Security Act (TDPSA)

The Texas Data Privacy and Security Act is a statewide consumer data privacy law that governs how businesses collect, use, and share personal data of Texas residents. It was enacted via House Bill 4 in 2023 and became effective on July 1, 2024, with some provisions phased in later.

Key facts

- **Effective date:** July 1, 2024 (core provisions)
- **Codified in:** Texas Business & Commerce Code, Chapter 541
- **Enforcement:** Exclusive authority of the Texas Attorney General; no private right of action
- **Universal opt-out mechanism effective:** January 1, 2025
- **Penalties:** Up to about $7,500 per violation (civil penalties)

Scope and who it covers

TDPSA applies to entities that conduct business in Texas or offer products or services consumed by Texas residents and process or sell personal data, with broad reach even without a revenue or data-volume threshold. Small businesses (as defined by the U.S. Small Business Administration) are generally exempt, though they must obtain consent before selling sensitive data.

Certain entities and data types are excluded, including state agencies, GLBA-regulated financial institutions, HIPAA-regulated entities and data, nonprofits, and higher-education institutions, among others.

Consumer rights

Texas residents acting in an individual or household context gain several rights over their personal data, including the right to:

- Confirm whether a controller is processing their personal data
- Access and obtain a copy of that data
- Correct inaccuracies in personal data
- Delete personal data in certain circumstances
- Opt out of:
    - Targeted advertising
    - Sale of personal data
    - Certain profiling producing legal or similarly significant effects

From January 1, 2025, consumers can also use “universal opt-out mechanisms” (like browser or device signals) to communicate their opt-out choices.

Business obligations

Covered “controllers” must:

- Limit collection to what is adequate, relevant, and reasonably necessary for disclosed purposes
- Provide clear, accessible privacy notices describing categories of data, purposes, sharing, and consumer rights
- Implement reasonable administrative, technical, and physical safeguards for personal data
- Obtain opt-in consent for processing sensitive data (e.g., precise geolocation, children’s data, certain biometric or health data)
- Conduct and document data protection assessments for high-risk processing such as targeted ads, sales of personal data, or profiling with significant effects

Processors acting on behalf of controllers must follow instructions, maintain confidentiality, assist with security and assessments, and meet contract requirements similar to those in other state privacy laws.

Enforcement and remedies

The Texas Attorney General has exclusive authority to investigate and enforce TDPSA. Before bringing an action, the AG must provide a notice and 30-day cure period, during which the business can remedy the violation and provide written assurances. Failure to cure or repeated violations can lead to civil penalties (up to roughly $7,500 per violation), injunctions, and recovery of attorneys’ fees and costs. There is no private right of action for consumers.

Relationship to other privacy laws

Substantively, TDPSA resembles other comprehensive state privacy laws (like those in Virginia and Colorado) but is notable for:

- Broad applicability based on doing business in Texas, not just revenue or data-volume thresholds
- Explicit exemption and tailored treatment for small businesses
- Exclusive AG enforcement and mandatory cure period
- Early adoption of a universal opt-out mechanism requirement

Together, these features position TDPSA as a significant part of the evolving U.S. patchwork of state consumer data privacy regulations.