Akin®

Texas Enacts Data Privacy and Security Act

July 31, 2023

Reading Time : **8 min**

By: Natasha G. Kohne, Joseph Hold

On June 18, 2023, Texas enacted the **Texas Data Privacy and Security Act (TDPSA)**, joining the rapidly growing list of U.S. states with comprehensive data privacy laws.[1] The statute will take effect on July 1, 2024, except for the right of consumer-designated agents to submit requests, which takes effect on January 1, 2025. The TDPSA is one of the more unique state privacy laws, but still borrows elements from Virginia's Consumer Data Protection Act (VCDPA) and California's Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA).

Key Provisions

- *Very Broad Scope* - unlike other states that apply revenue thresholds and volume of data processed to determine applicability, 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.
- *Expanded Definition of Personal Data* - in a rare change from other state data privacy laws, the definition includes pseudonymous data when the data is applied with other information that reasonably links the data to an identified or identifiable individual.
- *Dark Patterns Prohibited* - similar to privacy laws in California, Connecticut and Colorado, the TDPSA bans use of dark patterns (user interfaces designed to subvert user autonomy).
- *Small Businesses (Mostly) Exempt* - small businesses are exempt unless they sell sensitive data, in which case they must obtain consumer consent in advance.

- *Specific Privacy Policy Disclosure* - controllers who sell sensitive or biometric data must include specific, verbatim disclosures in their privacy notices.
- *Data Protection Assessments (DPAs)* - the law requires controllers to conduct DPAs for certain processing activities, providing factors controllers must consider to weigh the benefits against the risks of conducting the activity.

Who Must Comply with the TDPSA?

Much like other state laws, as well as the European Union's (EU) General Data Protection Regulation (GDPR), the TDPSA applies to "controllers" who determine the purpose and means of processing personal data, and "processors" who process that data on behalf of the controller.[2] The TDPSA is extremely broad, applying to any entity that:

- Conducts business in Texas or produces a product or service consumed by Texas residents.
- Processes or engages in the sale of personal data.
- Is not a small business as defined by the United States Small Business Administration.[3]

What Are the Notable Exemptions?

The TDPSA contains a variety of data-level exemptions common in this type of law, including: (1) protected health information under the Health Insurance Portability and Accountability Act (HIPAA);[4] (2) health records; (3) certain patient-identifying information and other information for research, health improvement or patient safety purposes; (4) personal data subject to the Fair Credit Reporting Act (FCRA); (5) data subject to the Family Educational Rights and Privacy Act (FERPA); (6) data subject to the Gramm-Leach-Bliley Act (GLBA); and (7) data processed or maintained as emergency contact information. The law also exempts personal data processed in the employment context, including data related to job applications and benefits.[5]

The law also features a number of entity-level exemptions, including: (1) nonprofits; (2) state agencies and political subdivisions; (3) financial institutions subject to GLBA; (4) covered entities and business associates governed by HIPAA; and (5) institutions of higher education. The TDPSA also specifically exempts electric utilities, power generation companies and retail electric providers.

What Is 'Personal Data' Under the TDPSA?

Texas has introduced a unique characterization of personal data, breaking with other states in favor of a more far-reaching definition. Under the TDPSA, personal data includes any information linked or reasonably linkable to an identified or identifiable individual, including sensitive data. This definition also 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."[6] While unique among state privacy law definitions of personal data, the TDPSA's inclusion of pseudonymous data plus other identifying information follows the GDPR. Additionally, certain consumer rights and controller duties do not apply to pseudonymous data where the controller "is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information."[7]

What Rights Do Texas Consumers Have?

Similar to other state privacy laws, the TDPSA excludes individuals acting in an employment or commercial context from the definition of "consumer," limiting the consumer rights extended under the law only to those residents of Texas acting in an individual or household context.[8] The law grants consumers a set of rights over their data akin to those in other state privacy laws, including the rights to: (1) **confirm** whether a controller is processing their personal data and access that data; (2) **correct** inaccuracies in their personal data; (3) **request deletion** of their data (whether the personal data was provided by the consumer or obtained about the consumer); (4) **obtain** a portable copy of their personal data; (5) **opt out** of processing for the purposes of targeted advertising, sale of personal data or profiling; and (6) **appeal** a controller's refusal to take action on a consumer request to exercise their rights.[9] The appeals process must be conspicuously available and "similar to the process for initiating action to exercise consumer rights."[10] Consumers also have the right to designate another person to serve as their agent to opt out of processing on the consumer's behalf[11], and as previously mentioned, this right takes effect on January 1, 2025, as opposed to the July 1, 2024 effective date for the rest of the law.[12]

Controllers under the TDPSA have 45 days to respond to a consumer request, extendable by an additional 45 days when reasonably necessary and with consumer notification.[13]

What Obligations Do Controllers and Processors Have?

The TDPSA contains requirements for both controllers and processors, similar to those found in other state privacy laws but with some unique additions.

Controller Requirements:

- **Data Minimization**: Controllers are required to limit personal data collection to what is relevant and reasonably necessary to the purposes for processing that data that the controller disclosed to the consumer.[14]
- **Data Security**: Controllers must implement and maintain reasonable administrative, technical and physical safeguards for protecting the confidentiality and integrity of personable data.[15]
- **Nondiscrimination**: Controllers must not process personal data in violation of state or federal laws prohibiting unlawful discrimination against consumers, and may not discriminate against consumers who exercise their rights under the TDPSA.[16]
- **Sensitive Data**: The TDPSA requires controllers to obtain a consumer's opt-in consent before processing their sensitive data. "Sensitive data" includes (1) data on racial or ethnic origin, religious beliefs, health diagnosis, sexuality or citizenship or immigration status; (2) genetic or biometric data processed to uniquely identify an individual; (3) personal data collected from a known child; and (4) precise geolocation data.[17] Collecting personal data from a known child (defined as an individual under 13 years of age) is considered sensitive data under TDPSA, which also specifies that any processing of sensitive data belonging to a known child must comply with the requirements of the Children's Online Privacy Protection Act (COPPA).[18] Unlike other state privacy laws, the TDPSA includes a defined term for "known child," which is a "a child under circumstances where a controller has actual knowledge of, or willfully disregards, the child's age."[19] Additionally, while small businesses are largely exempt from the TDPSA, they must still obtain consumer consent prior to selling sensitive data.[20]
- **Privacy Notice**: Similar to other state laws, controllers are required to provide consumers with a clear privacy notice, which includes (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) categories of data shared with third parties; (5) categories of third parties with whom the controller shares data; and (6) at least two methods for consumers to submit requests. However, unlike most other state laws, the TDPSA requires that controllers include a specific privacy disclosure if they sell sensitive data: "NOTICE: We may sell your sensitive personal data," or biometric data: "NOTICE: We may sell your biometric personal data."[21]

- **Data Protection Assessments**: Like Virginia, California and Colorado, the TDPSA requires controllers to conduct and document DPAs for certain processing activities. These activities include any processing that might present a heightened risk of harm to consumers, as well as: (1) processing for targeting advertising; (2) sale of personal data; (3) processing for certain types of profiling; and (4) processing sensitive data.[22]

Processor Requirements: Processors are required to follow controller instructions and assist controllers with meeting their obligations, including: (1) responding to consumer rights requests; (2) data security and breach notification; and (3) conducting and documenting data protection assessments.[23] As in other state laws, the TDPSA requires a contract to govern the controller-processor relationship that establishes clear instructions for processing the data, the nature and duration of the processing, the type of data to be processed and the rights and obligations of both parties.[24]

Who Enforces the Law?

California remains the only state privacy law so far with a private right of action, as the TDPSA grants the Texas Attorney General (AG) exclusive enforcement authority. The AG may initiate civil investigative demands and request any relevant DPAs from the controller.[25] The AG provides a 30-day cure period, which does not sunset.[26] For violations that are not cured, the AG may seek up to $7,500 in civil penalties per violation.[27] The law also mandates that the AG provide controllers, processors and consumers with information on their rights and responsibilities on the AG's website, along with an online portal for submitting complaints.[28]

With the addition of one of the largest states in the union, and the momentum behind state privacy laws showing no signs of slowing, businesses should prepare to face scrutiny from an

increasing number of regulators. Even companies that have made progress aligning their data practices with other privacy laws in the U.S. or EU should carefully consider the Texas law's broad applicability and unique elements to ensure compliance before the July 1, 2024 effective date.

Learn about the other State Laws in our State Data Privacy Law Series, as well as our *CCPA Litigation and Enforcement Report*:

1. **Virginia Consumer Data Protection Act: What Businesses Need to Know**
2. **Colorado Privacy Act: What Businesses Need to Know**
3. **Connecticut Data Privacy Act: What Businesses Need to Know**
4. **Utah Consumer Privacy Act: What Businesses Need to Know**
5. **Iowa Data Protection Act: What Businesses Need to Know**
6. **Key Takeaways from Akin's CCPA Litigation and Enforcement Report**

---

1 As of the date of this article, comprehensive state privacy laws have been enacted in California, Utah, Colorado, Connecticut, Virginia, Iowa, Indiana, Tennessee, Montana, Texas and Oregon. Delaware is expected to pass its law soon.

2 Texas Data Privacy and Security Act, Tex. Gen. Laws §§ 541.001(8), (23) (2023).

3 *Id*. § 541.002(a).

4 "HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and their implementing regulations (codified at 45 C.F.R. parts 160 and 164).

5 Id. § 541.003

6 Id. § 541.001(19).

7 Id. § 541.106(c).

8 Id. § 541.001(7).

9 Id. § 541.051(b).

10 Id. § 541.053(a).

11 Id. § 541.055(e).

12 Id. § 7(b).

13 Id. § 541.052(b).

14 Id. § 541.101(a)(1).

15 Id. § 541.101(a)(2).

16 Id. § 541.101(b)(2).

17 Id. § 541.001(29).

18 Id. § 541.001(17).

19 Id. § 541.101(b).

20 Id. § 541.107(a).

21 Id. § 541.102(b), (c).

22 Id. § 541.105(a).

23 Id. § 541.104(a).

24 Id. § 541.104(b).

25 Id. § 541.153(a).

26 Id. § 541.154(1), (2).

27 Id. § 541.155(a).

28 Id. § 541.152(1), (2).

Categories

Cybersecurity & Information Security

State Privacy Policy

Privacy & Cybersecurity

Consumer Data Protection