FAQs for Businesses as Texas Passes Consumer Privacy Legislation

Insights
7.03.23

Texas became the latest state to pass comprehensive consumer data privacy and security legislation when Governor Abbot signed the Texas Data Privacy and Security Act into law on June 18. It will require businesses to take several compliance steps by July 1, 2024, including updating website privacy notices, implementing a process for consumers to exercise rights under the Act, updating contracts with vendors acting as data processors, and conducting data protection assessments. Here are answers to your most pressing questions about how this impacts your business – and what you need to do to comply.

1. When Will the Law Become Effective?

The Texas Data Privacy and Security Act (TDPSA) will be effective on July 1, 2024, except for the Act's provisions that permit a consumer to designate an authorized agent to act on the consumer's behalf to opt out of the processing personal data and exercise of other rights under the Act. That provision takes effect on January 1, 2025.

2. Does the TDPSA Apply to Your Business?

The TDPSA's obligations to consumers only apply to an individual or 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; and
- is not a small business as defined by the United States Small Business Administration (although these entities are still subject to the TDPSA's prohibition against the sale of sensitive personal data without receiving prior consent from the consumer).

3. Does the Law Apply to Employment or Business-to-Business Situations?

As with most other states' data privacy laws (California being the exception), the TDPSA does not apply to employment or B2B data. **The Act specifically excludes an "individual acting in a commercial or employment context."**

This includes "data processed or maintained in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third

employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role."

4. Are Other Organizations Excluded From Coverage?

The TDPSA also excludes from its coverage state agencies, political subdivisions, nonprofit organizations, institutions of higher learning, electric utilities, power generation companies, other retail electric providers, and institutions and data subjects covered by the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act.

5. How Does the TDPSA Define "Personal Data"?

The Act defines "personal data" as "any information, including sensitive data, that is linked or reasonably likeable to an identified or identifiable individual." The term includes pseudonymous data "when it is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual" but does not include "deidentified data or publicly available information."

6. Can Individuals Sue for Violations of TDPSA?

No. The Act vests exclusive authority to enforce its provisions with the Texas Attorney General. The TDPSA specifically provides that it "may not be construed as providing a basis for, or being subject to, a private right of action" for a violation of its provisions or any other law. Individuals may, however, submit complaints to the Texas Attorney General which could cause issue a civil investigative demand.

7. What Consumer Rights Does the TDPSA Grant?

Following the trend of recent states, the TDPSA creates rights for consumers regarding their personal data, allowing them to:

- confirm whether a controller is processing their personal data and to access the personal data;
- correct inaccuracies in their personal data, considering the nature of the data and the purposes of the processing of the data;
- delete personal data provided by or obtained about them;
- if the data is available in a digital format, obtain a copy of their personal data that they previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows them to transmit the data to another controller without hindrance; or
- opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of a decision made by the controller concerning them that results in the provision or denial by the controller of the following: financial and lending

services; housing, insurance, or health care services; education enrollment; employment opportunities; criminal justice; or access to necessities, such as food and water.

8. What Obligations Do Covered Entities Have Related to Responding to Requests?

Controllers must establish two or more secure, reliable methods to allow consumers to submit a request to exercise their consumer rights under the TDPSA and provides certain factors those methods must consider. A controller may not require a consumer to create a new account to exercise their rights under the TDPSA but may require they use an existing account. The Act likewise requires any controller that maintains a to provide a method on the website for to submit requests for information required to be disclosed under the act.

Controllers must respond to a request "without undue delay," which cannot be later than 45 days after receipt of a request. The controller may extend the response period by an additional period once when reasonably necessary, so long as it informs the consumer of the extension (and reason for it) within the initial 45-day response deadline. The controller shall provide information in response to a request free of charge at least twice annually per consumer but may charge a reasonable fee where the request from a consumer is manifestly unfounded, excessive, or repetitive.

A controller is not required to respond to a request if unable to authenticate the request using commercially reasonable efforts and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the request. If denied, the controller must establish a process for the consumer to appeal a controller's refusal to take action on a request.

9. What Type of Privacy Notice Must Businesses Provide?

The TDPSA requires controllers to provide consumers with a reasonably accessible and clear privacy notice regarding the processing and sharing of personal data and how a consumer may exercise their consumer rights under the Act. This includes:

- the categories of personal information processed;
- the controller's purpose of processing the personal data;
- categories of personal data shared with third parties;
- the categories of third parties with whom consumer's data is shared; and
- a description of the methods required under the Act through which consumers can submit requests to exercise their consumer rights.

Controllers that engage in the sale of sensitive personal data must provide the following notice: "**NOTICE: We may sell your sensitive personal data**" which must be posted in the same location and in the same manner as the privacy notice.

Similarly, controllers that engage in the sale of biometric data must include the following notice: "**NOTICE: We may sell your biometric personal data**" in the same location and in the same manner as the privacy notice.

Controllers that sell personal data to third parties or process personal data for targeted advertising must "clearly and conspicuously" disclose that process and the way a consumer may opt out of it.

10. Do Businesses Need to Conduct a Data Protection Assessment?

Controllers must conduct and document a data protection assessment (DPA) of each of the data processing activities of personal data. The DPA must describe the processing of personal data for purposes of targeted advertising; the sale of personal data; the 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 to consumers; 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; and other substantial injury to consumers; the processing of sensitive data; and any processing activities involving personal data that present a heightened risk of harm to consumers.

In addition, a controller's data protection assessment must:

- identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce the risks; and
- factor into the assessment the use of deidentified data, the reasonable expectations of consumers, the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed.

11. Are There Additional Duties for Processors?

The TDPSA requires processors to comply with the instructions of controllers and assist them with meeting and complying with their duties imposed under the Act. Contracts between a controller and a processor must include clear instructions for processing data, the nature and purpose of processing, the type of data subject to processing and duration thereof, the rights and obligations of both parties.

The Act further requires that contracts between controllers and processors ensure that each person processing personal data is subject to a duty of confidentiality with respect to a consumer's data, and that the processor delete or return all personal data to the controller as requested after the provision of the service is completed.

As with similar laws enacted recently, processors must make available to the controller, on reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with the requirements of the Act, allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data.

12. What Should Businesses Do in the Meantime?

Even though July 1, 2024, may seem far down the road, compliance will not be quick work – so the time to begin to adapt your practices is now. If you are subject to the TDPSA, you should take immediate action to develop a roadmap for compliance and begin executing on the plan. Compliance with the TDPSA will take time and resources, so plan accordingly. Consider starting with a gap assessment of your current data collection and privacy practices, as that will help identify immediate versus your long-term priorities.

Completing a data inventory may be the next step, the results of which would feed into the drafting of compliant privacy notices and data protection assessments required by the Act. If your company is already compliant with other consumer privacy laws, you should consult your privacy counsel to determine what additional of differing requirements you may have to comply with the TDPSA.

Need More Help?

With the help of Fisher Phillips' Consumer Privacy Team, your steps towards compliance can be fast-tracked. We are prepared to assist your organization with TDPSA compliance from day one.

For further information, contact your Fisher Phillips attorney, the author of this Insight, or any attorney on the firm's Consumer Privacy Team. Fisher Phillips will continue to monitor any obligations and enforcement efforts and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Service Focus

Privacy and Cyber

Related Offices

Dallas

Houston