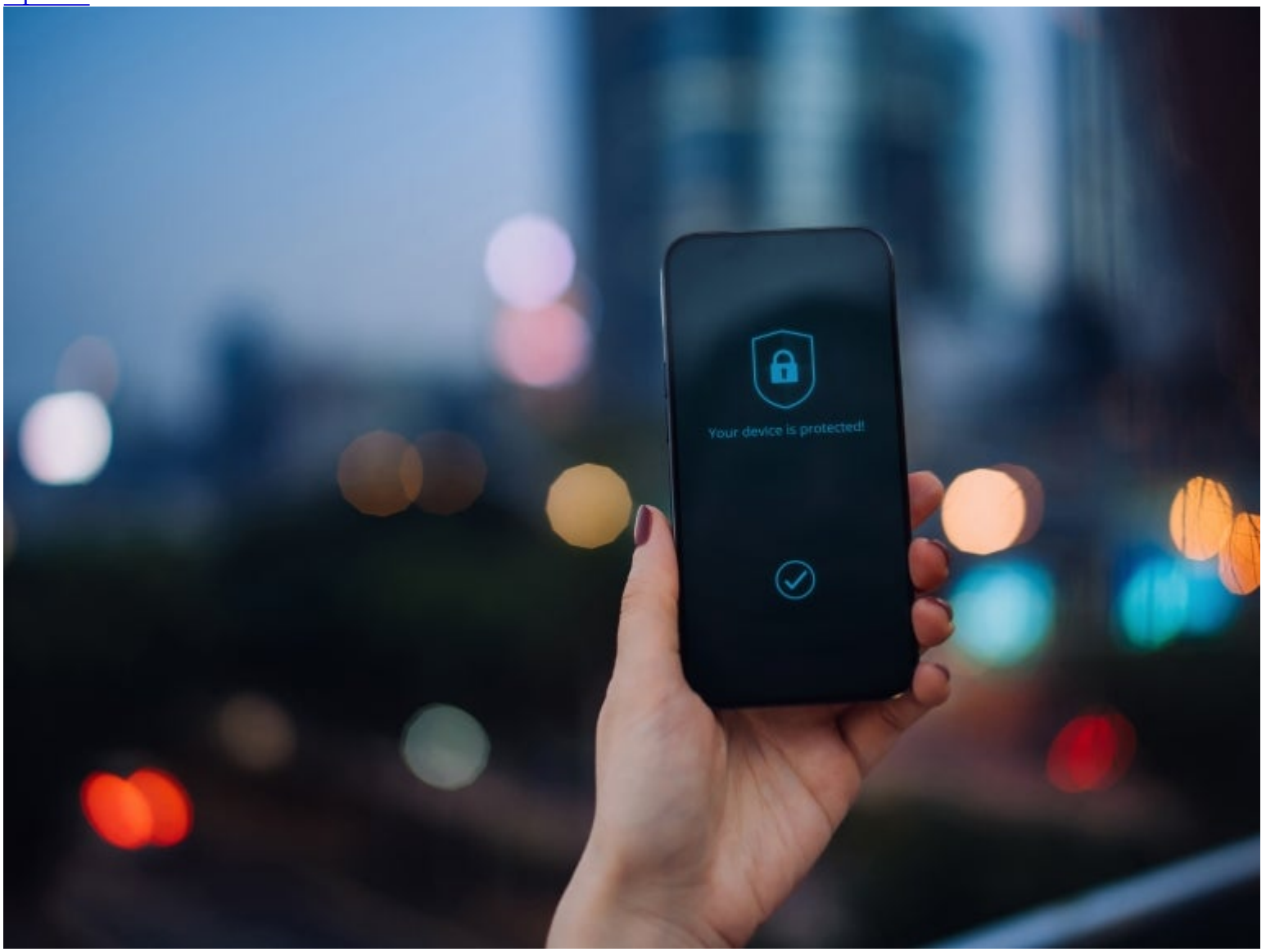
Updates



Texas Governor Greg Abbott signed the Texas Data Privacy and Security Act (TDPSA) into law on June 18, 2023. The comprehensive privacy and data security law will go into effect on July 1, 2024. The law and legislative history are available here.

We previously covered the TDPSA as it made its way through the Texas House of Representatives. The TDPSA largely follows the structure and terminology found in similar privacy and data security laws in Virginia and Colorado. Specifically, the TDPSA requires various disclosures around the collection and processing of personal data, provides consumers with rights to their data, requires opt-outs for certain data processing, and imposes obligations on controllers and processors, including honoring global opt-out signals. According to Texas State Representative Giovanni Capriglioni, who authored the original House Bill 4 on which the TDPSA is based, the TDPSA is intended to be business friendly by, among other things, exempting small businesses, not including

employee or business-to-business (B2B) data, placing enforcement solely with the Texas attorney general, and providing a period of 30 days to cure certain violations.

This Update provides an overview and summary of the main aspects of the TDPSA. It also provides recommendations on how companies that may be subject to the TDPSA can prepare for compliance.

Scope and Applicability

The TDPSA Applies to Businesses Inside and Outside of Texas

The TDPSA applies to any entity that satisfies all of the following:

- Conducts business in the state of Texas or produces a product or service consumed by the residents of the state of Texas.
- Processes or engages in the sale of personal data.
- Is not a "small business," as defined by the U.S. Small Business Administration (SBA).

The scope and applicability of the TDPSA differ from many existing comprehensive consumer privacy laws in a few ways. First, the TDPSA has broader applicability than many existing comprehensive consumer privacy laws because it applies not only to non-Texas entities conducting business in Texas but also to companies whose products or services are "consumed" by Texas residents. While phrased differently than other privacy laws (Virginia and those based on it), it has similar impact by pulling in businesses that are not located in Texas but process the personal information of Texas residents (through a "consumption" lens).

Second, instead of requiring a static revenue or consumer threshold like Virginia's Consumer Data Protection Act (VCDPA) or California's Privacy Rights Act (CPRA), the TDPSA uses guidelines established by the SBA, which are defined by law and tailored to each industry.

However, even entities that do not qualify as "small businesses" still must obtain consumer consent for the sale of sensitive personal data (TDPSA Section 541.107). This provision is unique to the TDPSA, capturing businesses of all sizes that process or engage in the sale of sensitive data if they are based in Texas or if Texas residents consume services or products from them.

The TDPSA Contains Various Exceptions

The TDPSA contains exceptions with respect to both entities and data types. The TDPSA excludes the following six different entities:

- Nonprofit organizations.
- Institutions of higher education.
- State agencies.
- Electric utility and power generators.
- Covered entities or business associates governed by the Health Insurance Portability and Accountability Act (HIPAA).
- Financial institutions subject to the Gramm-Leach-Bliley Act (GLBA).

The TDPSA also exempts 17 different data types, such as data regulated by the Family Educational Rights and Privacy Act (FERPA) and protected health information, as defined under HIPAA.

Similar to the approaches taken in other states, the TDPSA also excludes de-identified data and publicly available information from its definition of personal data.

Obligations

Data Rights

In line with many other comprehensive consumer privacy laws, the TDPSA provides Texans the following rights to their personal data: (1) access to their personal data; (2) correction of inaccuracies in their personal data; (3) deletion of personal data provided or obtained about them; (4) a copy of their personal data and transmission of it to another controller (referred to in some other privacy laws as "portability") if the data is available in a digital format; and (5) the ability to opt out of the sale, targeted advertising, and profiling in furtherance of a decision that produced a legal or similarly significant effect concerning them. Consumers must be provided with at least two methods to exercise these rights.

The consumer rights outlined in the TDPSA do not apply to pseudonymous data where the controller is able to demonstrate that any information necessary to identify the consumer is kept separate and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

Further, any provision of an agreement that attempts to waive or limit a consumer's right described in Section 541.051 through 541.053 of the TDPSA is recognized to be contrary to public policy and unenforceable.

Sale of Data

The definition of "sale" in the TDPSA is broader than this term under certain state laws and includes sharing, disclosing, or transferring personal data for monetary or other valuable consideration. However, the definition excludes data that is (1) transferred as an asset in the context of a merger or acquisition, (2) disclosed to an affiliate or a processor (referred to in some privacy laws as a "service provider") processing the data on the controller's behalf, and (3) disclosed for purposes of providing a product or service requested by the consumer (akin to the consumer direction exemption in other privacy laws like California's).

Privacy Obligations

Controllers subject to the TDPSA are required to disclose the following in their external-facing privacy policies: (1) the categories of personal data processed; (2) the purpose of the processing; (3) how consumers can exercise their rights; (4) the categories of personal data that the controller shares with third parties, if any; (5) the categories of third parties, if any, with whom the controller shares personal data; and (6) whether the controller sells personal data or processes personal data for targeted advertising. Like Virginia and Colorado, the TDPSA focuses on "targeted advertising" rather than adopting the CPRA's concept of "sharing" personal data in the "cross context behavioral advertising" or CCBA context (sharing is not a defined term under the TDPSA). The TDPSA also requires controllers to specifically state whether they sell sensitive personal data or biometric data, requiring them to include one or both of the statements (as applicable):

- "NOTICE: We may sell your sensitive personal data."
- "NOTICE: We may sell your biometric personal data."

These disclosures must be posted in the privacy notice. For controllers that process biometric data, be mindful that Texas also has the Capture or Use of Biometric Identifiers law (CUBI), which places additional disclosure, processing, and retention obligations on companies that collect and process biometric information. Under the TDPSA, controllers must also get consent to collect and process sensitive data.

The TDPSA also requires controllers to recognize and respect universal opt-out mechanisms for the purposes of opting out of the sale of personal data and targeted advertising. Unlike the rest of the TDPSA, this requirement does not become effective until January 1, 2025.

Controllers must also enter into written contracts with their processors that contain similar provisions required under other comprehensive consumer privacy laws. In addition, processors must enter into written contracts containing the same obligations imposed on the processor regarding personal data with any subprocessors they engage. Unlike the California privacy regulations, the TDPSA does not impose specific contractual obligations on the disclosure of personal data to third parties.

Controllers are also required to perform and document data protection assessments prior to a number of processing activities, including, but not limited to (1) the processing of personal data for targeted advertising purposes, (2) the sale of personal data, (3) the processing of personal data for certain profiling purposes, (4) the processing of sensitive data, and (5) any processing activities involving personal data that present a heightened risk of harm to consumers. The TDPSA contains requirements for how a data protection assessment must be performed, and a controller must make such assessments available to the Texas attorney general pursuant to a civil investigative demand.

Enforcement

The TDPSA does not include a private right of action, and the Texas attorney general has exclusive authority to enforce the TDPSA. Controllers and processors will have a 30-day cure period to remedy any violations of the TDPSA, but if such a violation is not remedied, the Texas attorney general may impose a civil penalty of up to $7,500 per violation. The TDPSA provides that the Texas attorney general's office must provide a complaint mechanism on its website, as well as provide controller and processor responsibility guidance in line with the TDPSA.

Similar to other state laws, the TDPSA requires companies to offer an appeal process when consumer requests are denied. Controllers must also provide consumers with information on how to lodge a complaint with the Texas attorney general.

The TDPSA does not call for the promulgation of any regulations, so the law will stand on its own, and any ambiguities will be ironed out as the Texas attorney general enforces the law. The regulations accompanying California and Colorado's privacy laws may also serve as a resource where more prescriptive guidance is sought, provided they do not conflict with the TDPSA.

How To Prepare

Companies that have already taken steps to comply with existing comprehensive consumer privacy laws will have a head start when it comes to developing a compliance program for the TDPSA, as many of the TDPSA's requirements align with those under other state laws.

Companies should conduct a data inventory to determine what personal data is being collected and what processing operations are taking place if they have not already done so. This is imperative for, among other things, accurate disclosures in the privacy policy, as well as timely compliance with consumer rights requests, under the TDPSA. As part of a thorough data inventory, companies should also take inventory of vendor/processor contracts and ensure those contracts are updated appropriately to include necessary restrictions and obligations set out in the TDPSA.

Companies should plan to update their external-facing privacy notices, and they may need to provide just-in-time privacy notices and implement opt-out notices for sales, targeted advertising, and the processing of sensitive data. They will also need to implement a way to intake and process consumer rights requests, including access and portability.

For assistance in preparing for the TDPSA, please consult with experienced privacy counsel.

Authors

Elijah Roden

Associate
ERoden@perkinscoie.com 214.259.4929

Pranav Bethala

Associate
PBethala@perkinscoie.com 214.965.7736

Explore more in

Privacy & Security Technology Transactions & Privacy Law Retail & Consumer Products

Related insights

Update

FERC Meeting Agenda Summaries for November 2024

Update

Ninth Circuit Rejects Mass-Arbitration Rules, Backs California Class Actions