

Buchanan



HigginbothamTM
Insurance and Financial Services



What to Know About the Texas Data Privacy and Security Act (TDPSA)

EFFECTIVE DATE: JULY 1, 2024

TABLE OF CONTENTS

WHO MUST COMPLY? 02

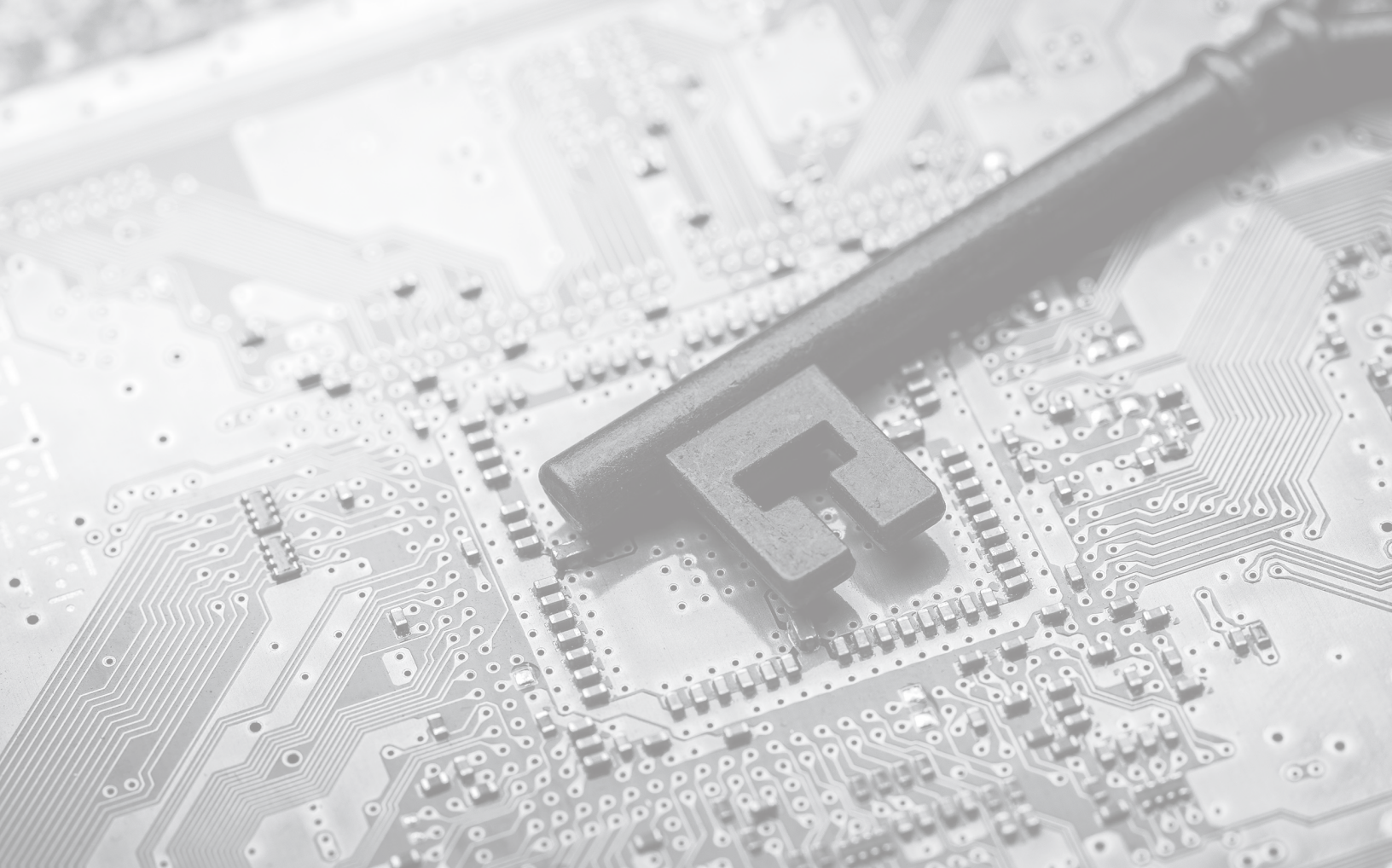
Terminology
Privacy Notice

CONSUMER RIGHTS 04

ROLE OF A PROCESSOR AND THE CONTROLLER/PROCESSOR CONTRACT 06

Data Protection Assessments
Enforcement





EXECUTIVE SUMMARY

On June 18, 2023, Texas became the 11th state in the U.S. to enact comprehensive data privacy legislation. Governor Greg Abbott signed HB 4, known as the Texas Data Privacy and Security Act (TDPSA). This act sets data collection, processing, and disclosure guidelines for consumer-facing companies doing business in Texas. The law will take effect on July 1, 2024, aligning the state with the broader national trend toward increased data protection.

Fourteen states have enacted “comprehensive” data privacy laws, granting consumers rights over how their personal data is collected and used. Some laws are currently in effect, while others, like Texas, take effect later this year. Several states are considering similar laws, with more expected to pass in 2024.

This guide provides an in-depth analysis of Texas data privacy laws, examining the current regulatory landscape and its implications for businesses operating in the state.



WHO MUST COMPLY?

Almost any consumer-facing company doing business or selling to residents in Texas is subject to the TDPSA. The TDPSA applies to a broader range of companies than most other recently adopted state privacy laws by encompassing any for-profit entity or individual that (1) does business in Texas or produces a product or service consumed by Texas residents and (2) processes or engages in the sale of personal data. Certain regulated entities and SBA small businesses are exempt.¹

Unlike other states' similar privacy laws, the TDPSA is not limited to organizations processing the personal data of a minimum number of state residents (commonly 100,000) or those deriving substantial revenue from personal data sales.

Terminology

The TDPSA uses the same definitions for the parties to which the law applies as are used in other state privacy laws (except California) and the EU's General Data Protection Regulation. These definitions include:

Controller: individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data.

Process: an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

Processor: a person that processes personal data on behalf of a controller.

¹ Exemptions include state government entities, nonprofits, entities subject to federal financial or health care regulation, higher education, electric utility or subject to Texas utilities regulation. Certain types of data are also excluded including health, clinical trial, credit, and student data if subject to certain federal and state regulations. TDPSA also does not apply to an individual acting in a commercial or employment context.

Privacy Notice

The TDPSA requires controllers to publish a privacy notice that is reasonably accessible and clear. The notice must disclose extensive information about the sources, types, purposes, disclosure, protection, and retention of personal data.

Disclosures similar to other state privacy laws:

- Categories of personal data processed by the controller, including any sensitive data.
- Purpose for processing personal data: Data collection and usage must align with the disclosed purposes to the consumer. A controller should outline its purposes in the privacy notice in a way that sets a baseline for how it intends to use the data while providing leeway for reasonable future expansion.

Disclosures similar to other state privacy laws:

- How consumers may exercise their rights, including information on appealing a controller's decision concerning the consumer's request.
- Categories of personal data that the controller shares with third parties.
- Categories of third parties with whom the controller shares personal data (specific third-party identities are not required).
- Clear and conspicuous right to opt-out from personal data use for sales or targeted advertising² if applicable.

- How consumers can submit requests to exercise their rights, including opt-outs and opt-ins if applicable. (Generally, there should be two different ways to submit a request to exercise a right, with at least one available via the controller's website.)

Disclosures different from some other state privacy laws:

- *If a controller sells sensitive data*, the notice must state:

“NOTICE: We may sell your sensitive personal data.”

If a controller sells biometric data, the notice must state:

“NOTICE: We may sell your biometric personal data.”

- *Opt-out from sales and targeted advertising.* Clear and conspicuous disclosure that personal data is sold or used for targeted advertising and the process for opt-out.
- *Right to appeal the denial of the exercise of consumer rights.* The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights.

² “Targeted advertising” means displaying to a consumer an advertisement that is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. Targeted advertising does not include an advertisement based on:

(1) Activities within a controller's own websites or online applications;
(2) A consumer's current search query, visit to a website, or online application; or
(3) Responding to the consumer's request for information or feedback.

Also excluded is the common practice of using personal data solely for measuring or reporting advertising performance, reach, or frequency.




Review Privacy Policy

CONSUMER RIGHTS

For the most part, the consumer rights established in the TDPSA are substantially similar to those in many other state privacy laws, including the specific rights, the methods for exercise, and the time periods for the controller to respond. These basic rights include:

- Confirmation of whether a controller is processing the consumer's personal data and accessing the personal data.
- Correction of inaccuracies in the consumer's personal data.
- Deletion of personal data provided by or obtained about the consumer. Note, however, that the TDPSA allows the controller to retain personal data that is still needed for internal operations that are reasonably aligned with a consumer's expectations.
- If the data is available in a digital format, the right to obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance.
- Opt-in required for processing sensitive data, which is defined to include:
 - Personal data 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 (under age 13); or
 - Precise geolocation data.
- Opt-out required for processing personal data for purposes of:
 - Targeted advertising;
 - The sale of personal data; or
 - Profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.
- Processing personal data only for disclosed purposes. Explicit informed consent is required for any other purpose.
- Non-discrimination for exercising consumer rights.



A controller generally must establish two or more secure and reliable methods for consumers to exercise their rights. These methods should align with how consumers normally interact with the controller, the need for secure communications, and the controller's ability to authenticate the person making the request. The controller must respond to a request within 45 days, with a permitted 45-day extension if reasonably necessary and the consumer is informed about the delay.

Other rights, while not unique, are less common, including:

Right to opt out of certain "profiling." A consumer has the right to opt out of having their personal data used for profiling that will be used in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer. Profiling is defined as "solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements [emphasis added]."

Opt-out preference signal. For opt-out from sales of personal data and targeted advertising (but not from automated profiling with a substantial effect), a controller must recognize as an "authorized agent" acting on behalf of a consumer an opt-out technology including "a link to an Internet website, an Internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt out of the processing." To be recognized in Texas, the technology must be user-friendly and require an affirmative choice by the consumer (i.e., not use a default setting).

Right to appeal. Texas consumers have a reasonable time to appeal if the controller declines the consumer's request to exercise a right. (Note that the controller must provide its justification for the refusal within 45 days of receiving the request.) The controller has 60 days to respond to the appeal. If the controller denies an appeal, the controller must provide an online mechanism through which the consumer may contact the attorney general to submit a complaint.

Special protections for deidentified data. Deidentified data refers to data that cannot reasonably be linked to an identified or identifiable individual or a device linked to that individual. When a controller possesses deidentified data, they must take reasonable measures to ensure that the data cannot be associated with an individual. Additionally, they must publicly commit to using and maintaining the deidentified data without attempting to reidentify it. Any recipient of the deidentified data must be contractually obligated to comply with the provisions outlined in the relevant chapter. If a controller discloses pseudonymous or deidentified data, they are responsible for monitoring compliance with contractual commitments and taking appropriate steps to address any breaches of those commitments.



ROLE OF A PROCESSOR AND THE CONTROLLER/PROCESSOR CONTRACT

All comprehensive state privacy laws require a written agreement between the controller and processor with very similar provisions. In turn, a processor is required to have the same requirements in a written contract with any subprocessor. The TDPSA recognizes that it is sometimes challenging to distinguish whether a person is acting as a controller or processor, emphasizing a context-dependent determination based on the responsibilities of the parties involved in a data processing activity.

The TDPSA identifies the duties and contract requirements of a processor to include:

- Assisting the controller in responding to consumer rights requests.
- Assisting the controller in complying with the requirement to process personal data securely.
- Providing the information the controller needs to conduct and document data protection assessments.
- Ensuring that each person processing personal data on behalf of the processor (e.g., employee, subcontractor) is subject to a duty of confidentiality.
- At the controller's direction, deleting or returning all personal data to the controller after the processing service is completed, unless retention is required by law.

- Making available to the controller, on reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with the TDPSA.
- Allowing, and cooperating with, reasonable assessments by the controller or the controller's designated assessor.
- Engaging any subcontractor pursuant to a written contract that requires the subcontractor to meet the same statutory and contractual requirements as the processor with respect to the personal data.

The TDPSA provides a practical alternative to the requirement of assessing the compliance of its processors. The processor may engage a "qualified and independent assessor" to conduct an assessment of the processor's policies and technical and organizational measures using an appropriate and accepted control standard and assessment procedure and provide a report of the assessment to the controller on request.

Data Protection Assessments

Controllers are also required to conduct a “data protection assessment” before implementing a new or changed business process involving any of the risks identified above for any of the following:

- 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 to consumers;
 - 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; or
 - Other substantial injury to consumers.
- Processing of sensitive data
- Any processing activities involving personal data that present a heightened risk of harm to consumers

The data protection assessment is a formal, documented process where the controller weighs the benefits of the proposed data collection and use against the potential risks to consumers’ rights and reasonable expectations. The controller may take into account security safeguards and other mitigating procedures that can be feasibly deployed and effectively used to reduce risks. Examples of safeguards are technical and organizational measures such as access controls, encryption of sensitive data, and an active data retention/destruction program. The Texas attorney general has the power to require a controller to disclose a data protection assessment under an investigative demand.

Enforcement

TDPESA does not provide for a private right of action. The Texas attorney general is responsible for enforcing the law and may seek civil penalties of up to \$7,000 per violation. Before bringing an action, the attorney general must provide an alleged violator a 30-day notice to rectify the violation by notifying the consumer, changing internal policies as needed, and providing documentation to the attorney general as to how the violation was rectified.

For any inquiries about data privacy laws, please contact the authors.



MICHAEL G. MCLAUGHLIN

Buchanan Ingersoll & Rooney
Cybersecurity and Data Privacy Practice
Group Co-Leader
michael.mclaughlin@bipc.com
202 452 5463



SUE C. FRIEDBERG

Buchanan Ingersoll & Rooney
Cybersecurity and Data Privacy Practice
Group Co-Leader
sue.friedberg@bipc.com
412 562 8436



COREY HUEY

Higginbotham Insurance
and Financial Services
Cyber & Digital Asset Risk Practice Leader
chuey@higginbotham.com
281 543 9867