Texas Data Privacy and Security Act Summary

On June 18, 2023, Governor Greg Abbott (R) signed HB 4, the "Texas Data Privacy and Security Act" into law. The Act's provisions take effect on July 1, 2024. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Texas Data Privacy and Security Act** applies to a person that: (a) conducts business in the state or produces a product or service consumed by residents of the state; (b) processes or engages in the sale of personal data, and; (c) is not a small businesses as defined by the United States Small Business Administration.
Covered Data	***"Personal data"***: any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual. The term 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. "Personal data" does not include deidentified data or publicly available information. ***"Sensitive data"***: a category of personal data that includes: (a) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status; (b) genetic or biometric data that is processed for the purpose of uniquely identifying an individual; (c) personal data collected from a known child; (d) precise geolocation data.
Key Definitions	***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. "Consent" may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. ***"Dark Pattern":*** a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice, and includes any practice the Federal Trade Commission refers to as a dark pattern. ***"De-Identified Data"***: data that cannot reasonably be linked to an identified or identifiable individual, or a device linked to that individual. ***"Pseudonymous Data"***: any information that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual. ***"Targeted Advertising"***: displaying an advertisement to a consumer in which the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. ***"Sale of Personal Data"***: the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include: (a) the disclosure of personal data to a processor that processes the personal data on the controller's behalf; (b) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; (c) the disclosure or transfer of personal data to an affiliate of the controller; (d) the disclosure of information that the consumer and did not restrict to a specific audience; or (e) the disclosure or transfer of personal data to a third party as an asset that is part of a merger or acquisition.

Consumer Rights	• **Access:** A consumer has the right to confirm whether a controller is processing the consumer's personal data and to access such personal data. • **Correction:** A consumer has the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data. • **Deletion**: A consumer has the right to delete personal data provided by or obtained about the consumer. • **Portability:** If the data is available in a digital format, a consumer has 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 Out Rights**: A consumer has the right to opt out of the processing of the consumer's personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
Business Obligations	• **Responding to Consumer Requests**: A controller shall respond to a consumer without undue delay, but not later than 45 days of receipt of a request. The controller may extend the response period by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, provided the controller informs the consumer of the extension with the initial 45-day response period along with the reason for the extension. If a controller declines to act regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to act and provide instructions for how to appeal the decision. A consumer has the right to a free response at least twice annually per consumer. The controller bears the burden of demonstrating the manifestly unfounded, excessive, repetitive, or technically unfeasible nature of any denied requests and may charge the consumer a reasonable fee to cover such administrative costs or decline to act on such requests. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken in response to the appeal and provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint. • **Data Minimization**: A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. • **Avoid Secondary Use**: A controller shall not process personal data for a purpose that is neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent. • **Data Security**: To protect the confidentiality, integrity, and accessibility of personal data, a controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue. • **No Unlawful Discrimination:** A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any consumer rights. • **Transparency**: A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes: (a) the categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller; (b) the purpose for processing personal data; (c) how consumers may exercise their consumer rights, including the process by which a consumer may appeal a controller's decision with regard to the consumer's request; (d) if applicable, the categories of personal data that the controller shares with third parties; (d) if applicable, the

	categories of third parties with whom the controller shares personal data, and; (e) a description of the methods through which consumers can submit requests to exercise their consumer rights. • **Disclosure**: If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process.
Data Protection Impact Assessments	A controller shall conduct and document a data protection impact assessment of each of the following processing activities involving personal data: (a) the processing of personal data for the purposes of targeted advertising; (b) the sale of personal data; (c) the processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of: (i) unfair or deceptive treatment of or unlawful disparate impact on consumers; (ii) financial, physical or reputational injury to consumers; (iii) 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; (iv) other substantial injury to consumers; (d) the processing of sensitive data, and (e) any processing activities involving personal data that present a heightened risk of harm to consumers. Data protection assessments must identify and weigh the 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: (a) the use of deidentified data; (b) the reasonable expectation of consumers; (c) the context of the processing; and (d) the relationship between the controller and the consumer whose personal data will be processed. A controller must make a data protection assessment available to the attorney general pursuant to a civil investigative demand. A data protection assessment is confidential and exempt from public inspection and copying. A single data protection assessment may address a comparable set of processing operations that include similar activities. A data protection assessment conducted by a controller for the purpose of compliance with other laws or regulations may constitute compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.
Controller / Processor Distinction	• **A processor shall adhere to the instructions of a controller and shall assist the controller** in meeting or complying with the controller's duties or requirements, including: (a) assisting the controller in responding to submitted consumer rights requests by using appropriate technical and organizational measures, as reasonably practicable, insofar as this is reasonably practicable, taking into account the nature of processing and the information available to the processor; (b) assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor's system, taking into account the nature of processing and information available to the processor; and (c) providing necessary information to enable the controller to conduct and document data protection impact assessments. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. • The contract must require that a processor: (a) ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data (b) at the controller's direction, delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law; (c) make available to the controller, on reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with this law's requirements; (d) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; and (e) engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

Exceptions and Exemptions	• A controller may disclose pseudonymous data or de-identified data with an exercise of reasonable oversight to monitor compliance with any contractual commitments and shall take appropriate steps to address any breaches of those contractual commitments. • The Texas Data Privacy and Security Act shall not be construed to restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government authorities or cooperate with law-enforcement agencies; (c) prepare for and defend legal claims; (d) provide a product or service specificallyrequested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of a consumer before entering into a contract; (e) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and in which the processing cannot be manifestly based on another legal basis; (f) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; (g) preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security; and (h) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored or governed by an institutional review board or a similar independent oversight entity. • Data exempt from the Texas Data Privacy and Security Act includes:, protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, and COPPA. • Organizations exempt from the Texas Data Privacy and Security Act includes: nonprofit organizations, institutions of higher education, a covered entity or business associate governed by HIPAA and HITECH, and institutions subject to the Gramm-Leach Bliley Act.
Enforcement	• The Texas Data Privacy and Security Act does not provide the basis for a private right of action to violations of this Act. • **Right to Cure**: The attorney general has exclusive authority to enforce the Texas Data Privacy and Security Act. The attorney general may initiate an action and seek an injunction and a civil penalty not to exceed $7,500 per violation. Before initiating any action, the attorney general shall provide a controller or processor 30 days' written notice identifying specific provisions being violated.