BRACEWELL

INSIGHTS

Now There Are 10: The Texas Data Privacy and Security Act

June 21, 2023

*By: **Lucy Porter** and **Anissa L. Adas***

Texas has joined the nine[1] other states that have comprehensive data privacy laws after Governor Greg Abbott signed the Texas Data Privacy and Security Act (the "TDPSA"). Subject to exemptions,[2] the TDPSA applies to any entity (labeled controller under the Act) that (1) conducts business in Texas or produces a product or service consumed by residents of Texas; (2) processes or engages in the sale of personal data; and (3) is not a small business as defined by the US Small Business Administration.[3] The SBA defines a small business as a business with fewer than 500 employees. The law goes into effect on July 1, 2024.

For those familiar with data privacy laws, the TDPSA by and large follows the model of Virginia with respect to the rights granted to consumers and the obligations placed on controllers. The applicability provision is unique, as are several other provisions: (a) a requirement to post prescribed notices regarding the sale of sensitive personal data and biometric personal data; (b) a thirty day cure period that requires more from the alleged violator than a statement that the alleged violation has been cured; and (c) a prohibition on sales of personal data by small businesses without the prior consent of the consumers. Also note the additional deadline of January 1, 2025, by which controllers must be able to support universal opt-out signals.

For those not familiar with data privacy laws, read on to learn more about the provisions of the TDPSA.

Definition of Personal Data

Unlike California, the TDPSA does not apply to data processed or maintained in the employment context ("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 party, to the extent that the data is collected and used within the context of that role"). Additionally, the TDPSA exempts data "processed or maintained and is necessary to retain or administer benefits for another individual that relates to an individual [in the employment context] and used for the purposes of administering those benefits."

Under the TDPSA, the definition of personal data is general, defined as "any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual." Surprisingly, the TDPSA definition of sensitive data is more limited than similar laws and only 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 processed for the purpose of uniquely identifying an individual; (c) personal data collected from a known child; or (d) precise geolocation (i.e., accuracy within a radius of 1,750 feet).

In addition to the exemption for data in the employment context, the TDPSA exempts data in categories related to health information, patient information, research information protected under HIPAA or other similar regulations, data used in activities regulated by the Fair Credit Reporting Act, data protected under the Driver's Privacy Protection Act, data regulated by the Federal Educational Rights and Privacy Act, data covered by the Farm Credit Act, and emergency contact information.

Consumer Rights and Process

As with other comprehensive data privacy laws, the TDPSA grants consumers (a) the right to confirm whether a controller is processing the consumer's personal data and to access the personal data; (b) the right to correct inaccuracies; (c) the right to delete; (d) the right obtain a copy of data available in a digital format; and (e) the right to opt out of processing for purposes of (1) targeted advertising, (2) sale of personal data, or (3) profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.

Most entities will be required to maintain two methods by which consumers may submit consumer requests, at least one of which is through its website. These methods are in addition to the universal opt-out method noted above.

Controller Duties

As with other data privacy laws, controllers have a duty to limit the collection of personal data "to what is adequate, relevant, and reasonably necessary in relation to the purpose for which that personal data is processed;" and "shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices." Controllers, as defined by the TDPSA, must perform data protection assessments only in the limited circumstances set out in the Act. Contracts with processors (a person that process personal data on behalf of a controller) must include requirements to protect consumers' personal data. Controllers are required to publish a privacy notice that meets specified requirements.

Steps to Take in Preparation of July 1, 2024

Given the breadth of the applicability provisions, it is likely that the TDPSA will apply to a large number of Texas-based entities, but a first step is to determine the applicability to your business. A second critical analysis is understanding the personal data your organization collects

and, importantly, how the personal data is used, shared, disclosed, and sold, and to whom. With these assessments in hand, you will be ready to begin taking steps to comply with the TDPSA.

Bracewell lawyers are available to assist you in these and other tasks in this growing patchwork of state data privacy compliance.

---

[1] Other states with comprehensive data privacy are California, Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Utah, and Virginia,

[2] The TDPSA exempts the following types of entities (a) state agencies or political subdivisions of the state, (b) financial institutions subject to Gramm-Leach-Bliley, (c) covered entities or business associates governed by the privacy, security, and breach notification rules under HIPAA and HITECH, (d) nonprofit organizations, (e) institutions of higher education, and (f) electric utilities, power generation companies, and retail electric providers.

[3] Subject to a prohibition against sales of certain personal data in certain situations.