texas and oregon's comprehensive privacy law is coming into effect: time to prepare for enforcement actions

Susan Kohn Ross, Lucy Plovnick, & Stacey Chuvaieva
MSK Client Alert

July 1, 2024

On July 1, 2024, Texas and Oregon's comprehensive data privacy laws took effect. The Texas Data Privacy and Security Act (TDPSA) was signed into law on June 18, 2023. Most[1] of its obligations will go into effect on July 1 and will likely be vigorously enforced. The Oregon Consumer Data Privacy Act (OCDPA), signed into law on July 18, 2023, also goes into effect today.

Texas Attorney General Ken Paxton has already established "a team that is focused on aggressive enforcement of Texas privacy laws." According to his statement released on June 4: "[t]he team is poised to become among the largest in the country focused on enforcing privacy laws."

The TDPSA can apply to your business if you:

- Conduct business in or produce a product or service consumed by residents of the State of Texas.
- Process or engage in the sale of personal data.
- Are not a small business as defined by the Small Business Administration.

Notably, there is ***no particular threshold limit*** for the applicability of the TDPSA as in similar privacy laws enacted in other states, and even exempt entities, such as a "small businesses" are prohibited from selling sensitive personal data without consumer consent.

The TDPSA does not apply to state agencies, a financial institution or data subject to Title V, the Gramm-Leach-Bliley Act, institutions of higher learning, electricity utilities and providers, healthcare providers overseen by the U.S. Department of Health and Human Services, and nonprofits.

attorneys

Stacey Chuvaieva, CIPP/US/E

Lucy Holmes Plovnick, AIGP, CIPP/US

Susan Kohn Ross

practice areas

cybersecurity and privacy

Unlike the California Privacy Rights Act of 2020 (CPRA), the TDPSA does not apply to employees or contractors, as it exempts any individuals "acting in a commercial or employment context."

Overall, the TDPSA, in many ways, parallels Virginia's and Colorado's state privacy laws, but it also has particular requirements that could trigger changes to the privacy policies already in place at businesses in order to ensure compliance.

The key aspects of the TDPSA are:

Consumer Rights. Similar to comprehensive privacy laws in other states, the TDPSA provides the rights to delete, correct, and access consumer's personal data, and to opt out of sales and targeted advertising. The TDPSA also gives consumers a right to opt out of "profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer" and must clearly and conspicuously disclose a consumer's right to opt out. Consumers will also have a right to appeal a denial of a data subject's request.

Required Notices. One aspect of the TDPSA is a requirement to post notices for the sale of sensitive personal data in the same location and in the same manner as a privacy notice. If a business "sells" sensitive personal data or biometric personal data, the TDPSA requires inclusion of the following notice:

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

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

The TDPSA defines "sale of personal data" broadly, similar to the CPRA's definition of sale, covering "sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party."

Consent to Process Sensitive Data. The TDPSA requires all businesses to obtain consent before processing "sensitive" personal data. Personal data collected from a known child is considered a category of "sensitive data" and must be processed in accordance with such requirements.

Children & Willful Blindness. The TDPSA defines "known child," as a person under 13 years of age, where the business has actual knowledge of "or willfully disregards" the child's age. This definition parallels the Texas Securing Children Online through Parental Empowerment Act (SCOPE) signed into law on June 13, 2023. SCOPE similarly uses the willful blindness test, but defines a minor as a child under the age of 18. SCOPE also has a much more narrow application covering only digital service providers that enable social interactions, profile creation, and content sharing among users. A business which processes children's data in accord with the Children's Online Privacy Protection Act (COPPA) consent requirements will be deemed in compliance with the TDPSA.

los angeles
t 310.312.2000
f 310.312.3100

new york
t 212.509.3900
f 212.509.7239

washington, dc
t 202.355.7900
f 202.355.7899

Data protection Impact Assessment. The TDPSA mandates that controllers conduct and document data protection assessments for specific processing activities: processing personal data for targeted advertising, profiling, selling personal data, processing sensitive data, and any activity posing a heightened risk to consumers. These assessments must evaluate and balance the benefits of the processing activity against potential consumer risks, considering the safeguards in place.

Pseudonymous Data. Unlike other privacy laws, the definition of personal data includes pseudonymous data when the data is applied with other information that reasonably links the data to an identified or identifiable individual. At the same time, this term does not include deidentified data or publicly available information.

Dark Patterns. Similar to the privacy laws in California, Colorado and Virginia, the TDPSA prohibits use of dark patterns, defined as 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." Any consents obtained through the use of dark patters would not enforceable.

No Private Right of Action. The act vests enforcement powers only in the Texas Attorney General, and does not provide for a private right of action.

A 30-day Cure Period. The TDPSA does permit a 30-day cure period which, unlike under the CPRA, does not sunset.

Penalties. As mentioned, enforcement is exclusively vested in the Texas Attorney General's Office. In case of an uncured breach, the Texas Attorney General may initiate an action against the data controller and/or processor and recover up to $7,500 in civil penalties per violation. Unclear at this point is whether that means per consumer record, and presumably it does so that any fine would be substantial.

The TDPSA does not authorize the Texas Attorney General to promulgate regulations, so businesses and consumers will have to rely on enforcement of the law to clarify and shape further implementation. We are likely to see more action in this area in the upcoming months. Following his June 4th statement, the Texas Attorney General has issued letters notifying over one hundred companies of their failure to comply with Texas' newly enacted Data Broker Law.

Given what appears to be the intent of the Texas Attorney General towards rigorous enforcement, this is the right time to update privacy policies and make sure your processes and policies do not include anything which could be considered "willful blindness" in processing data, especially that of children.

Turning to the Oregon's law:

Scope. Unlike the Texas law, the OCDPA contains thresholds and applies only to the entities which during a calendar year: (i) control or process personal data of at least 100,000 Oregon consumers, other than personal data controlled or processed solely for the purpose of completing a payment transaction; or (ii) control or process personal data of at least 25,000 Oregon consumers and derive over twenty-five percent (25%) of their

annual gross revenue from the sale of personal information. However, its scope is potentially broader than other similar state privacy laws because it applies to entities that conduct business in Oregon or provide products or services to Oregon residents. Therefore, the law would apply to businesses that do not specifically target Oregon residents, but just make their services available in the state. Such a board definition likely includes anyone with a website that sells products or services. Nonprofits are also covered, but the OCDPA delays enforcement for nonprofit entities until July 1, 2025.

Overall, the scope of the OCDPA is similar to most other state privacy laws: the law expressly excludes personal data collected or processed from individuals acting in a "commercial or employment context" and does not cover data regulated by other privacy laws, such as the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act.

Interestingly, unlike similar state privacy laws, the OCDPA defines personal data broadly to include data "linked to or [] reasonably linkable to a consumer or to a device [that can be linked to a consumer.] [Emphasis added]"

In all other aspects, the OCDPA follows the requirements of similar state privacy laws.

Consumer rights. Consumer rights cover the rights to request confirmation regarding whether an entity is processing their personal data, obtain a copy of their data, correct inaccuracies, delete data, opt out of targeted advertising and profiling, and revoke consent to process their data, which must be honored within 15 days. Consumers will also have a right to appeal any decision made about their privacy requests. The OCDPA also contains broader disclosure requirements. When requested by a consumer, a covered entity must provide the list of all entities to which the controller has disclosed personal data, whereas other state privacy laws only require disclosing the categories of third parties with whom data was shared.

Children. The OCDPA also provides that covered entities must obtain the consumer's consent if the entity knowingly processes personal information of children 13-15 years old for the purposes of targeted advertising, sale of personal data, or profiling. Like the TDPSA, Oregon's law addresses the data collected by the entity that "willfully disregards" "whether, the consumer is at least 13 years of age and not older than 15 years of age[.]"

Enforcement. Penalties under the OCDPA are similar to those we described regarding the TDPS: Oregon's law provides no private right of action and is enforced by the Oregon Attorney General. The law also contains a thirty (30) day period to cure the violation(s) but that provision expires on January 1, 2026. The fines are similar to those under the TDPS: up to $7,500 per violation.

Feel free to give our Cybersecurity and Privacy team a call if you would like more information or assistance.

[1] Obligations regarding the processing of consumer privacy requests by authorized agents and recognition of Global Privacy Control go into effect January 1, 2025.