Better Call Your Privacy Attorney: 3 New State Privacy Laws Begin July 1, 2024

by Sara H. Jodka

On July 1, 2024, Florida, Oregon, and Texas will join California, Colorado, Connecticut, Utah, and Virginia by adding privacy laws governing the collection, use, and transfer of consumer personal data. Montana will follow suit effective October 1, 2024.

The new laws are similar to existing state data privacy laws in that they grant consumer protections and impose requirements on companies collecting, i.e., processing personal data. They also overlap in a number of ways, meaning companies that have privacy programs that comply with existing data privacy laws will not have to make significant changes to their existing programs to come into compliance. However, companies that may have to come into compliance for the first time will need to update their privacy policies and develop and implement new processes before July 1, 2024.

What Businesses Are Covered?

Understanding the unique nuances of each state's privacy laws is crucial. Businesses must discern the criteria that render these laws applicable and comprehend the necessary steps if their operations fall under their purview.

Texas

Starting with the broadest-reaching law, the Texas Data Privacy and Security Act (TDPSA) will apply to entities that (a) conduct business in Texas or offer products and services consumed by Texas residents and (b) process or sell personal data.

Unlike most state privacy laws that require compliance only if an entity collects personal data of a certain number of consumers or has gross annual revenue of a certain amount, the TDPSA applies to large businesses and expressly exempts small businesses (except those that process sensitive data) and nonprofits. This is a first-of-its-kind carve out.

So, what is an exempt small business for purposes of the TDSPA? According to the U.S. Small Business Administration (SBA), the standard varies by industry and is "usually stated in number of employees or average annual receipts," as outlined by the SBA in its Table of Size Standards. This means that entities that conduct business in Texas or offer products and services consumed by Texas residents will have to determine if they are exempt from the law as a "small business" or if they have to comply.

Regardless of size or revenue, the TDPSA will require all businesses to obtain opt-in consent prior to selling sensitive personal information, discussed more fully below.

Oregon

Oregon's Consumer Data Privacy Act (OCPA) will apply to persons/entities that conduct business in Oregon or produce products or services targeted to Oregon residents that either (a) control or process the personal information of at least 100,000 Oregon residents (excluding personal data processed for payment transactions) or (b) control or process the personal information of 25,000 Oregon residents and derive over 25% of its gross annual revenue from selling personal information.

Like Colorado's Privacy Act (CPA), the OCPA *will apply* to nonprofit organizations, though they will have *until July 1, 2025*, to comply with the OCPA.

Montana

The Montana Consumer Data Privacy Act (MCDPA) will apply to persons/entities that conduct business in Montana or produce products or services targeted to Montana residents and that either (a) process the personal information of 50,000 Montana residents or more (excluding personal data processed for payment transactions) or (b) that process the data of 25,000 or more consumers (who do not have to necessarily be Montana residents) and derive 25% of gross revenue from the sale of such data.

Florida

Florida's Digital Bill of Rights (FDBOR) is the narrowest as it will only apply to persons that (a) conduct business in Florida or produce products or services used by Florida individuals or households and (b) process or engage in the sale of personal data. Unlike other state consumer privacy laws, only a minimal number of large tech firms will be subject to the FDBOR as it only applies to data controllers that operate a business in Florida with annual gross revenue over 1 billion dollars and that either:

1. Make 50% or more of their revenue from selling online ads, including targeting advertising;
2. Operate a consumer smart speaker and voice command component service; or
3. Operate an app store with more than 250,000 apps.

However, like the TDSPA, the FDBOR will require any data controller to obtain express consent before selling an individual's sensitive information.

What Is Personal Data?

The Texas law defines "personal data" as "any information, including pseudonymous data and sensitive data," that can be reasonably linked to an individual. Other states have not expressly extended data subject rights to access, correct, delete, or port data to pseudonymized data, but the TDPSA does provide that such data subject rights will not be triggered if the entity holding the data can show that any information necessary to identify the consumer is separately stored and subject to technical and organizational controls that prevent it from accessing such information.

The Oregon law defines "personal data" to include "data, derived data, or any unique identifier" that is reasonably linkable to (a) a consumer or (b) to a device that is linkable to one or more consumers in a household. "Derived data" is not included in any other state privacy law, which means that the Oregon law likely creates new obligations that would extend compliance obligations and data subject rights to inferences about a consumer.

Under the MCDPA, "personal data" means any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual, including pseudonymous data when used by the entity in conjunction with additional information that reasonably links the data to an identified or identifiable individual.

What Is Sensitive Data?

The new laws include specific protections for sensitive data, including requiring consent before any sensitive data may be processed. This means that privacy notices will have to be updated to allow for implicit consent (where allowed) or a pop-up banner or similar technology placed on a website to allow a consumer to check a box indicating expressed consent at the point of collection, which is required in Texas.

In the TDPSA, "sensitive data" includes child data, precise geolocation information, genetic or biometric data, data of known children, precise geolocation data, and personal data revealing racial or ethnic origin, religious beliefs, citizenship and immigration status, and health status. The TDPSA requires a covered business to obtain consent before processing and/or selling sensitive data. In the event a covered business does sell sensitive data, the business must provide "**NOTICE: We may sell your sensitive personal data**" (and similarly, "**NOTICE: We may sell your biometric personal data**" in the event the business processing biometric data) in the same manner as the privacy notice.

The OCDPA defines "sensitive data" as data that reveals a consumer's racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis, sexual orientation, status as transgender or non-binary, status as a victim of crime, citizenship or immigration status, and child data. The OCDPA is like the Virginia Consumer Data Protection Act (VDPA) in that it requires that consumers opt in before their sensitive information can be collected/processed.

The MCDPA defines "sensitive data" as data that reveals a consumer's racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, information about a person's sex life, sexual orientation, or citizenship or immigration status.

Requirements

In an overly simplistic nutshell, covered entities are required to:

- Provide consumers with a clear privacy notice, including the categories of personal data to be processed, the purpose of processing personal data, how consumers may exercise their rights, categories of data shared with third parties, and categories of third parties with whom the company shares data;
- Limit personal data collection to what is reasonably necessary for processing that data;
- Include contact information for consumers to submit requests regarding their personal data;
- Obtain consent from consumers before processing their sensitive data;
- Implement reasonable administrative, technical, and physical safeguards for protecting personable data;
- Conduct data protection assessments for certain processing activities, including targeting advertising, sale of personal data, processing of sensitive data, and any processing that might present a heightened risk of harm to consumers; and
- Enter into data processing agreements with any third parties processing personal data on their behalf.

The new laws also give their state residents several familiar rights, including the right to:

- Confirm whether a controller is processing and accessing personal data;
- Correct inaccuracies in their personal data;
- Delete personal data provided by or obtained about the consumer;
- Obtain a copy of their personal data in a portable and readily usable format, if available; and
- Opt out of processing personal data for targeted advertising, the sale of personal data, or its use for profiling.

Additionally, the OCPA grants individuals the right to know the specific third parties to whom a data controller discloses their personal data, which will augment standard data subject rights to access, correct, delete, and port data.

Exclusions

There are other exclusions as most laws do not apply to state government entities, nonprofits (except Oregon), HIPAA-covered entities and business associates, higher educational institutions (public or private), utility service providers, and Gramm-Leach-Bliley Act-regulated entities and data, but they may.

Next Steps

Companies already in compliance with existing privacy laws will have a familiar roadmap to follow for compliance, though they will need to accept data privacy requests from consumers residing in those states, update their process for managing privacy requests to include them, and ensure they align with the requirements specific to each state they fall under.

However, companies having to comply with these data privacy laws for the first time must create new policies and processes to ensure compliance. The easiest thing to do is to start by focusing on requirements that the data privacy laws have in common. Covered entities must conspicuously post a privacy notice that explains to consumers what personal data is collected, how it is used, with whom it is shared if it is sole, and how they can exercise their privacy rights. Businesses will then need to devise clear and reliable processes for receiving and responding to consumer privacy requests. Businesses collecting sensitive personal data must ensure that they obtain consent prior to collecting such data and that they have completed a data protection assessment addressing the uses of the data.

Given that the collection of personal data must be limited to what is necessary to achieve the purpose for which it was collected, a good place to start is with a data audit that identifies what data the company collects, how it collects it, why it collects it, and what it does with it. Once covered entities understand what data they need to collect and why, they can develop the required privacy notice and other policies, such as a data retention policy with a precise data retention period to ensure personal data is not retained longer than needed.

While each state law has some requirements that overlap, the reality is that state law has compliance requirements specific to that state, and each law must be reviewed and understood to ensure compliance.

Beyond 2024

In addition to Florida, Montana, Oregon, and Texas, new consumer privacy laws in Delaware, Iowa, Nebraska, New Hampshire, New Jersey, and Tennessee will become effective in 2025, and Indiana and Kentucky laws will take effect in 2026.

ABOUT THE AUTHORS

Sara H. Jodka (Member, Columbus) is a certified privacy professional with CIPP-US, CIPP-E, and CIPM certifications. Sara assists companies of all sizes with their data privacy and cybersecurity privacy needs. She can be reached at sjodka@dickinsonwright.com, and for more information, please refer to her bio.