June 17, 2024

Just in Time for the 4th of July, New Privacy Laws Effective in Texas, Florida, and Oregon

by Tatum Andres , John M. Brigagliano , Gregory P. Silberman

On July 1, 2024, three more U.S. state privacy regulations will take effect. While these laws align with many of the principles established by other state privacy laws, they also introduce unique compliance requirements specific to each state's legislative framework.

As the regulatory landscape continues to evolve, businesses must stay informed and proactive in their compliance efforts. This overview highlights key aspects of forthcoming legal changes that may require updates to your privacy compliance work.

The Texas Data Privacy and Security Act (TDPSA) imposes significant compliance obligations for businesses, excluding small businesses, that operate in Texas or provide products and services to Texas residents.

One notable aspect of the TDPSA is the aggressive enforcement approach by the Texas Attorney General. According to a recent press release, the Texas Attorney General, Ken Paxton, has established a dedicated team within its Consumer Protection Division focused on enforcing privacy laws, including the TDPSA. The TDPSA establishes guidelines for how controllers must handle, verify, and respond to consumer privacy requests. Controllers with websites must provide a mechanism for consumers to submit data privacy requests online. For controllers that operate exclusively online and collect personal information directly from consumers, providing an email address for these requests is sufficient.

The TDPSA requires that organizations establish a process allowing consumers to appeal a controller's refusal to act on a data rights request. The appeal process must be clearly accessible and similar to the process for submitting privacy rights requests. Controllers are required to notify consumers in writing about the actions taken in response to appeals, provide the reasons for their decisions, and inform consumers how they can contact the attorney general to file a complaint.

Beginning January 1, 2025, covered organizations must acknowledge universal opt-out mechanisms, such as the Global Privacy Control, enabling consumers to opt out of the sale of their personal data and its use in targeted advertising (this requirement becomes effective on July 1, 2024, under the Colorado Privacy Act—see below). Under the TDPSA, personal data is defined broadly to include any information that can be linked to an identified or identifiable individual, encompassing pseudonymous and sensitive data. This distinguishes it from other U.S. privacy laws by specifically including pseudonymous data, which requires additional information to

attribute it to a specific individual, though the requirements for handling pseudonymous data are relatively limited. A controller that sells personal data or uses it for targeted purposes has the additional obligation to "clearly and conspicuously disclose" such processing and how consumers can exercise their opt-out rights.

The law sets out requirements for data minimization, security, and consumer rights like other state laws, and includes specific notice and opt-in consent requirements for the sale of sensitive or biometric data that applies to all businesses – including those that would otherwise be exempt as a small business. Sensitive data, as defined by the TDPSA, includes information that reveals racial or ethnic origin, religious beliefs, mental or physical health diagnoses, sexuality, citizenship or immigration status, genetic or biometric data used for identification, data collected from known children, and precise geolocation data. Processing sensitive data is subject to stricter regulations and generally requires obtaining consent from the relevant party. Controllers that sell sensitive data or biometric personal data must post a notice in the same location and manner as the privacy notice, and these respective notices must include the following language:

- For sale of sensitive data, "NOTICE: We may sell your sensitive personal data."
- For sale of biometric data, "NOTICE: We may sell your biometric personal data."

The Oregon Consumer Privacy Act (OCPA) also introduces significant changes. What sets Oregon's privacy law apart is the introduction of a new privacy right not found in other state comprehensive privacy laws: the right to request from a controller a list of specific third parties, excluding natural persons, to whom the controller has disclosed personal data. The controller can respond by naming the third parties that have received either the requesting consumer's personal data or any personal data. This new right necessitates that companies keep a detailed list of specific third parties rather than merely describing categories of recipients. This emphasizes the importance of maintaining a comprehensive data inventory that includes the types of personal data collected, the reasons for collection, and the parties to whom it is disclosed.

The OCPA applies to entities controlling or processing data of 100,000 Oregon residents or 25,000 residents if over 25% of revenue comes from selling personal information. "Sensitive data"[1] includes the categories set forth in most other comprehensive data privacy laws. However, the OCPA introduces unique elements, such as including data revealing transgender or nonbinary status as part of a broader definition of sensitive, granting consumers the right to request a consumer-specific or general third parties their data is shared with, and including "derived data" within the definition of personal data.

The OCPA, similar to the California Privacy Rights Act (CPRA), provides a narrower exemption for financial institutions compared to other states' privacy laws, which generally provide a full exemption for entities considered financial institutions under the federal Gramm-Leach-Bliley Act (GLBA). As a result, financial institutions subject to the GLBA may now need to comply with the OCPA in addition to the CPRA.

The Florida Digital Bill of Rights (FDBR) differs from other US privacy laws by specifically targeting large tech platforms, focusing on businesses with global gross annual revenues exceeding $1 billion that are involved in activities such as selling ads online as a primary business model, operating smart speakers, or running a large app store.[2] The law emphasizes consumer opt-out rights for data collected via voice and facial recognition and

includes specific provisions for children's online privacy. The FDBR also prohibits the use of certain device features for surveillance without active consumer authorization and mandates specific data retention schedules.

Violations of the FDBR, similar to those under the Colorado Privacy Act (CPA), are classified as deceptive trade practices. Once the Attorney General notifies an organization of violations in writing, a 45-day cure period may be granted, allowing the organization to address the issues and implement preventive measures without facing penalties. Unlike some of the other state privacy laws, the FDBR does not include a provision to sunset the cure period after a year or two. The cure period does not apply if a violation involves a known child.

Civil penalties under the law may be tripled for any violation involving a Florida child who the online platform has actual knowledge is under 18 years of age.

The Florida law also allows parents to exercise rights on behalf of their children (i.e., act as a child's agent) and contains an age-appropriate design code for services predominantly accessed by children (those under 18). This is similar to Connecticut's Data Privacy Act (CDPA), which allows a child's parent or legal guardian to exercise rights on the child's behalf when the child's personal data is being processed.

The FDBR provides that consumer opt-out out rights should be made available on the company's website. The law gives consumers the right to confirm whether their data is processed, obtain a copy of their data, correct any inaccuracies related to their data, and delete their data. Under the FDBR, the data controllers are obligated to respond to the data subject requests within 45 days following the receipt of the request. If the request is complex, data controllers may extend this deadline by up to 15 days.

How The Three New Privacy Laws Stack Up Against Existing Regulations

Unlike the California Privacy Rights Act, the definition of "consumer" under the three above laws excludes individuals acting in a commercial or employment context, so business to business personal data and employee personal data do not fall within the scope.

The following chart highlights some of the other unique requirements under each of the new laws.

Requirement	Texas (TDPSA)	Oregon (OCPA)	Florida (FDBR)
Scope and Applicability	Businesses in Texas or companies providing products/services to Texas residents; exempts small businesses.	Processing data of 100,000 Oregon residents or 25,000 residents if over 25% revenue from selling personal info; includes nonprofits.	Businesses with annual revenue over $1 billion and a) 50%+ revenue from online ads, b) smart speakers and voice command services, or c) operate a large app store.
Consent Requirements (selected)	Opt-in consent for processing sensitive personal data.	Parental consent for profiling data from individuals aged 13-15.	Opt-in consent required for collection of data via voice and facial recognition.

Requirement	Texas (TDPSA)	Oregon (OCPA)	Florida (FDBR)
Sensitive Data	Broad definition of “personal data” includes pseudonymous data and sensitive data that can be reasonably linked to an individual.	Includes data revealing transgender or nonbinary status and status as a victim of a crime; past or present location within 1750 feet.	Specific provisions for online platforms targeting children (under 18); requires an affirmative opt-in prior to selling sensitive data, regardless of revenue.
Privacy Notices	Categories of personal data processed; purposes of processing; consumer rights exercise info; third-party data sharing; specific notices for sensitive/biometric data sale.	Clear information on processing activities; disclose third parties with whom data is shared.	Clear and concise privacy notices about data collection and processing activities.
Data Protection Assessments	Required for high-risk processing activities, targeted advertising, data sales, profiling, and sensitive data processing.	Required where processing activities are likely to present a heightened risk of harm to consumers; must be retained for five years.	Required for targeted advertising, sale of personal data, and profiling where there is a potential risk of harm to consumers.
Enforcement	Texas Attorney General enforcement; 30-day cure period; penalties up to $7,500 per violation; no private right of action.	Oregon Attorney General enforcement; 30-day cure period expiring January 1, 2026; penalties up to $7,500 per violation; no private right of action.	Florida Department of Legal Affairs and Attorney General enforcement; 45-day cure period; penalties up to $50,000, with treble damages for specific violations; no private right of action.

Businesses operating in these states should review these regulations carefully to ensure compliance by July 1, 2024. Also effective July 1, 2024, controllers subject to the Colorado Privacy Act (CPA) must recognize Colorado consumers' privacy preferences submitted through browser signals conforming to the Global Privacy Control (GPC) specification as requests to opt out of data sales or targeted advertising.

Looking ahead to the rest of the year, the Montana Consumer Data Privacy Act (MCDPA) and the Maryland Kids Code become effective on October 1, 2024.

Footnotes

[1] S.B, 619, 82nd Leg. Assemb., Reg. Sess. §1(18)(a) (Oregon 2023).

[2] Specifically, in addition to the $1 billion in global gross annual revenue, the business must satisfy at least one of the following: (1) derives 50% or more of its global gross annual revenues from the sale of advertisements online, including providing targeted advertising or the sale of ads online, (2) operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation; or (3) operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install. S.B. 262, § 501.702(9)(a)(1)-(6)(Florida 2023).