



Alerts

3 New State Privacy Regulations Take Effect on July 1, 2024, With Federal Legislation Still on the Horizon: Are You Ready to Comply?

June 24, 2024

Privacy, Cyber & AI Decoded

Over 18 states have now enacted comprehensive state privacy laws, three of which go into effect on **July 1, 2024**, in Texas, Florida, and Oregon, along with certain California Data Broker provisions.

We issued a [prior alert](#) with detailed information about several of these state privacy laws. Given the concerns about the lack of progress with the federal American Privacy Rights Act (APRA), we expect state enforcement of comprehensive privacy laws to continue to escalate.

Keep reading these new and important developments to ensure your organization complies.

Texas Data Privacy and Security Act (TDPSA): Texas Builds Out the Largest Privacy Enforcement Team

The TDPSA will take effect on **July 1, 2024**.

Texas Attorney General Ken Paxton is building out the “largest” Attorney General’s team to focus on the aggressive enforcement of privacy laws. According to Attorney General Paxton’s press release, his data privacy team will be focused on enforcing the following laws:

- TDPSA,
- Identify Theft Enforcement and Protection Act,
- Data Broker Law,
- Biometric Identifier Act,
- Deceptive Trade Practices Act, and
- two federal laws, the Children’s Online Privacy Protection Rule and the Health Insurance Portability and Accountability Act.

Paxton indicated that his aggressive enforcement would also apply to companies that are irresponsibly using personal or sensitive data in artificial intelligence (AI) or without required consent.

Attorneys

Sabrina Janeiro

Cathy Mulrow-Peattie

Jason J. Oliveri

J. Michael Paulino

Service Areas

Privacy, Security & Artificial Intelligence



What should companies do in response? Review your privacy notices, security protocols, and related privacy and security practices across your personal data and AI use cases to ensure you comply with the TDPSA.

Florida Digital Bill of Rights (FDBR)

The FDBR will take effect on **July 1, 2024**.

The comprehensive privacy portion of the statute has a narrower scope of applicability than other state laws. For **July 1**, understand if you fall within the threshold requirements of the FDBR:

- The FDBR applies only to entities deemed as “**Controllers**,” which are defined as for-profit legal entities that conduct business within the state of Florida, collect personal data from consumers, determine the purposes or means of the processing of personal data, have an annual global revenue of more than \$1 billion and meet one of the following criteria:
- Derive 50 percent of its global gross annual revenue from the sale of advertisements online;
- Operate a consumer smart speaker and voice command service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation; or
- Operate an app store or digital distribution platform with at least 250,000 different software applications for consumers to download and install.

A separate section of the bill related to the protection of children in online spaces, which applies to online platforms defined as social media platforms, online games, or online gaming platforms, will also take effect on **July 1, 2024**. This section more strictly regulates how these online platforms profile children, use children’s sensitive personal information, and share and sell children’s personal information. A child is defined as someone under 18 years of age.

Oregon Consumer Privacy Act (OCPA)

The Oregon Attorney General’s Office issued FAQs to assist businesses in complying with the OCPA, which will take effect on **July 1, 2024**. It emphasizes that controllers and companies must:

1. “Provide notice regarding the types of personal data the controller processes, the specific purpose(s) for processing data, whether and why the controller shares personal data with third parties, and information about how consumers can exercise their various rights (e.g., access, deletion) over their personal data.
2. Limit collection of personal data to what is adequate, relevant, and reasonably necessary for the specific purpose(s) for which the data is collected and processed (also known as “data minimization”).
3. Respond to requests to exercise consumer rights granted under the law.
4. Conduct assessments before processing personal data in a manner that presents a heightened risk of harm to consumers (called “Data Protection Assessments”). This includes processing personal data for the purposes of targeted advertising, sale, or profiling, and any processing of sensitive data.
5. Use reasonable safeguards to secure personal data.”

California Consumer Privacy Act (CCPA)

California data brokers subject to the state’s amended data brokerage registration law also have an upcoming compliance deadline of **July 1, 2024**.

Specifically, to comply with §7102 of the CCPA, covered entities must compile the number of requests to delete, correct, know, limit, and/or opt out of sale/sharing that they have received from consumers over the last calendar year. This information must be posted in their privacy policy by **July 1, 2024**, along with the median number of days it took the entity to provide a substantive response.



Will there be a Federal American Privacy Rights Act (APRA)?

Parties on both sides of the aisle have long recognized the need for a comprehensive federal privacy law. However, legislators are no closer to enacting one than they were in 2022 when we [reported](#) on the American Data Privacy and Protection Act (ADPPA)—the first of its kind to show any real promise.

Although it has been reported that a new discussion draft of the latest proposal, the APRA, will be heard by the full House Energy & Commerce Committee on June 27, it is not expected to advance. The main sticking points do not appear to have changed much over the years and relate to concerns about preemption, a private right of action, law enforcement, and how the law would affect small and medium-sized businesses. Stay tuned for additional updates on this topic.

Is your organization in compliance? View [Hinshaw's Privacy, Security, and Artificial Intelligence services](#) to learn how we can help you today.