CLIENT ALERTS & INSIGHTS

Three US State Data Protection Laws Set to Take Effect in Less Than Two Months

MAY 8, 2024

*Updated May 10, 2024
2023 saw a dramatic increase in states passing omnibus data protection laws. As the mid-point of 2024 arrives, effective dates also arrive. On July 1, 2024, the number of US states with broad, omnibus data protection laws in effect will nearly double-to a total of eight-greatly increasing the footprint of active data protection laws in the U.S.

Florida, Oregon, and Texas will join the ranks of the existing five U.S. state data protection laws that are in effect.

Tennessee-with a last minute amendment prior to passage-takes effect July 1, 2025. However, the last minute amendment did not update the date upon which the data protection risk assessments are required to cover. Tennessee's data protection risk assessment requirements apply to any data processing activities as of July 1, 2024. Businesses falling within the scope of Tennessee's data protection law should begin focusing on compliance efforts in preparation of next year's effective date.

Between 2025 and 2026, an additional nine U.S. states will have their data protection laws take effect as well, for a grant total of 17 effective state data protection laws.

To aid in the constant effort of keeping track of new U.S. state data protection laws, Benesch Friedlander Coplan and Aronoff and the Data Meets World blog now feature a "U.S. State Privacy Laws" landing page that offers a high level overview of all U.S. states with data protection laws in place and key requirements and takeaways from those laws.

The webpage offers a continuously updated snapshot of the U.S. state data protection landscape. To use the Data Meets World interactive U.S. Privacy Laws webpage, click here. Below, please find more information on the timing for when each state has data protection laws coming into effect and what businesses will be subject to the data protection laws of a given state.

Upcoming States

There are already five US states with data protection laws in effect: California; Colorado; Connecticut; Utah; and Virginia.

On July 1, 2024-less than two months away-that number will nearly double when Florida's, Oregon's, and Texas's data protection laws join and make it nine total states with data protection laws in effect.

Montana will make it nine when Montana's data protection law takes effect in October of this year.

As of now, nine additional states will come into effect between 2025 and 2026. Those nine states include Delaware, Indiana, Iowa, Kentucky, Maryland, Nebraska, New Hampshire, New Jersey, and Tennessee. There are also a number of states that are close to passing data protection laws through their respective state legislatures that will only add to the list as time goes on.

Scope and Applicability of U.S. State Data Protection Laws

All states set forth a prerequisite that only a business operating or doing business in the specific state is subject to the law. Unfortunately, the analysis does not stop there. Generally, a business must also meet certain "thresholds".

There are generally three thresholds that bring businesses into the scope of a U.S. State's data protection law: (1) annual, worldwide gross revenue (not just the revenue derived out of the applicable state); (2) the total collection of personal information from consumers in the applicable state; or (3) the collection and sale of the state's consumers' personal information.

Pertinent to the upcoming laws taking effect, Texas is unique in that they have **no** thresholds. Therefore, Texas's law will apply much more broadly to any business collecting any amount of Texas consumers' personal data.

In contrast, some states are narrower in applicability. Florida, for example, requires a business to hit a certain annual revenue threshold-$1 billion in annual gross revenue-**and** for one of the additional applicability thresholds to apply.

It is important to note that-to date-California is still the only U.S. state data protection law that applies to more than just consumer personal data. California's data protection law covers employee, job applicant, contractor, and business-to-business personal data within the scope of the law. The other U.S. state data protection laws broadly exempt out personal data collected in any employment context.

Below are the specific applicability thresholds that a business must meet before the July 1 effective data protection laws apply:

- Florida
  - $1 billion in gross, worldwide annual revenue; AND
    - 50% of gross, worldwide annual revenue from the sale of advertisements online; including targeted advertising; OR
    - Operates a consumer-facing smart speaker and voice command service connected to cloud computing services that are hands-free
  - Oregon
    - Processing 100,000 or more Oregon consumers' personal data; OR
    - 25% of gross, worldwide annual revenue from selling personal data and processing at least 25,000 Oregon consumers' personal data
  - Texas
    - Conducting business in Texas; AND
    - Processing or sell **any** amount of Texas consumers' personal data; AND
    - is not a small business as defined by Federal regulations

Check out the "U.S. State Privacy Laws" landing page for information on other US states already in effect and coming into effect over this year and years to come.

Conclusion

At a high level, U.S. data protection law was built on a foundation of "notice and choice". Businesses publish privacy policies and notices describing, at a high level, their data collection and use practices, and the informed consumer decides whether to continue interacting with that business.

While the new U.S. state data protection laws all build, and still largely rely, on the traditional privacy law foundation of "notice and choice," they've also added specific scenarios where the onus is on the business to take affirmative steps to proactively protect consumers or to enhance the choices and decision-making power those consumers have. As more U.S. states pass comprehensive data protection laws and such laws come into effect, more and more business will need to build-out substantive, data protection compliance programs.

Those programs will need to adaptable-as one business could be subject to multiple state laws and therefore must adapt to the nuanced differences-and will need to account for the different aspects of comprehensive data protection laws, such as (1) substantive privacy policies and notices; (2) consumer privacy right request policies and procedures; (3) reasonable, adequate technical,

organizational, and physical security measures; (4) vendor and contract management programs to flow through required contractual provisions when engaging data processors and service providers; and (5) regular audit procedures and programs.

The above list is not exhaustive of all a business would need to do under the applicable U.S. state laws; but it provides an example of the different requirements comprehensive data protection laws set forth-and the time it will take for business to build out compliant programs.

Businesses that have not previously dealt with comprehensive data protection law compliance will need to invest a significant amount of time in developing the required policies and procedures. Additionally, even if businesses have previously dealt with other-or former versions of-comprehensive data protection laws, they will need to conduct comprehensive reviews in order to account for specific nuances and differences in the laws.

As more states continue to implement their own variations of data protection laws and business' juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.