CLIENT ALERTS & INSIGHTS

Kentucky Governor Signs Kentucky Consumer Data Protection Act into Law

APRIL 10, 2024

Kentucky joins the growing trend of U.S. state data protection laws with well over a dozen now in place across the country.

Last year proved to be a huge year in U.S. state data protection law, ending with 13 U.S. states with comprehensive data protection laws on the books. And 2024 shows no sign of stopping or slowing that trend.

New Hampshire and New Jersey became the first two states in 2024 to pass omnibus data protection laws. Kentucky now joins the exponentially growing ranks of U.S. states with omnibus data protection laws in place, which a handful of other states poised to quickly add to the list as well.

The law itself follows in the mold of other U.S. state data protection laws, setting up the now familiar data controller and processor dynamic.

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 laws all build, and still largely rely, on the traditional privacy law foundation of "notice and choice," they've also added specific scenarios where affirmative actions must be taken to proactively protect consumers or to enhance the choices and decision-making power those consumers have.

With well over a dozen states now adding their own spin to this body of law, it can be hard to keep up.

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. That page has now been updated to add Kentucky to the list.

The new webpage offers a continuously up to date 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.

States and Effective Dates

2023:

- California
  - January 1, 2023
- Colorado
  - July 1, 2023
- Connecticut
  - July 1, 2023
- Utah
  - December 31, 2023
- Virginia
  - January 1, 2023

2024:

- Florida
  - July 1, 2024
- Montana
  - October 1, 2024
- Oregon
  - July 1, 2024
- Tennessee
  - July 1, 2024
- Texas
  - July 1, 2024

2025:

- Delaware
  - January 1, 2025
- New Hampshire
  - January 1, 2025
- Iowa
  - January 1, 2025
- New Jersey
  - January 16, 2025

2026:

- Indiana
  - January 1, 2026
- Kentucky
  - January 1, 2026

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. But it is not that simple. To be subject to the applicable state laws, the "do business in the state" prerequisite must be met, but a business must also meet certain "triggers".

There are generally three triggers 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.

Some states, like Florida and Utah, require a business to hit a certain annual revenue threshold **and** for one of the additional applicability thresholds to apply. This set up narrows the applicability of the data protection laws in Florida and Utah.

It is important to note that-to date-California is 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.

-
  - California
    - Over $25 million in gross, worldwide annual revenue; OR
    - Processing 100,000 or more California residents' personal data; OR
    - 50% of gross, worldwide annual revenue from selling personal data
  - Colorado
    - Processing 100,000 or more Colorado consumers' personal data; OR
    - Receiving any profit from selling personal data and processing at least 25,000 Colorado consumers' personal data
  - Connecticut
    - Processing 100,000 or more Connecticut consumers' personal data; OR
    - 25% of gross, worldwide annual revenue from selling personal data and processing at least 25,000 Connecticut consumers' personal data
  - Delaware
    - Processing 35,000 Delaware consumers' personal data (excluding, personal data processed solely to complete a payment transaction);
    - 20% of gross, worldwide annual revenue from selling personal data and processing at least 10,000 Delaware consumers' personal data
  - 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

- Indiana
  - Processing 100,000 or more Indiana consumers' personal data; OR
  - 50% of gross, worldwide annual revenue from selling personal data and processing at least 25,000 Indiana consumers' personal data

- Iowa
  - Processing 100,000 or more Iowa consumers' personal data; OR
  - 50% of gross, worldwide annual revenue from selling personal data and processing at least 25,000 Iowa consumers' personal data

- Kentucky
  - Processing 100,000 or more Kentucky consumers' personal data; OR
  - 50% of gross, worldwide annual revenue from selling personal data and processing at least 25,000 Kentucky consumers' personal data

- New Hampshire
  - Processing 35,000 New Hampshire consumers' personal data; OR
  - Over 25% of gross, worldwide annual revenue from selling personal data and processing at least 10,000 New Hampshire consumers' personal data

- New Jersey
  - Processing 100,000 or more New Jersey consumers' personal data; OR
  - Receiving any profit from selling personal data and processing at least 25,000 New Jersey consumers' personal data

- Montana
  - Processing 50,000 or more Montana consumers' personal data; OR
  - 25% of gross, worldwide annual revenue from selling personal data and processing at least 25,000 Montana consumers' personal data

- 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

- Tennessee
  - Processing 100,000 or more Tennessee consumers' personal data; OR
  - 50% of gross, worldwide annual revenue from selling personal data and processing at least 25,000 Tennessee consumers' personal data

- Texas
  - Conduct business in Texas; AND
  - Process or sell **any** amount of Texas consumers' personal data; AND
  - Are not a small business as defined by Federal regulations

- Utah
  - $25 million in gross, worldwide annual revenue; AND
  - Processing 100,000 or more Utah consumers' personal data; OR
  - 50% of gross, worldwide annual revenue from selling personal data and processing at least 25,000 Utah consumers' personal data

- Virginia
  - Processing 100,000 or more Virginia consumers' personal data; OR
  - 50% of gross, worldwide annual revenue from selling personal data and processing at least 25,000 Virginia consumers' personal data

Kentucky Data Protection Law Privacy Rights

Under the Kentucky Consumer Data Protection Act, consumers will have the following rights: (1) to confirm whether a business is processing the consumer's personal data, (2) to access the personal data a business holds about them; (3) to correct the personal data a business holds about them; (4) to have their personal data deleted; (5) to receive a summary of or a copy of the personal data held about them in a portable and usable form (data portability); (6) to opt-out of the sale of their personal information; (7) to opt-out of targeted advertising; and (8) to opt-out of profiling someone through solely automated means in furtherance of decisions with legal or similar effect (e.g., employment, benefits, etc.).

Additionally-in line with U.S. state data protection laws-Kentucky requires businesses to give consumers the right to appeal that businesses denial of a data privacy right request.

Like many other U.S. state data protection laws, the Kentucky Consumer Data Protection Act requires a business to obtain prior opt-in consent before collecting, using, or otherwise processing a consumer's sensitive personal data. "Sensitive personal data" under the Kentucky Consumer Data Protection Act is defined as any category of data identifying: (1) race, ethnicity, or religion; (2) mental or physical health; (3) sexual orientation; (4) citizenship or immigration status; (5) genetic or biometric data processed with the purpose of identifying an individual; (6) the personal data of a child (younger than 13); or (7) a person's precise geolocation (within a radius of 1,750 feet).

Enforcement of the Kentucky Consumer Data Protection Act

In line with the new U.S. state data protection laws, the Kentucky Consumer Data Protection Act does not provide individuals with a private right of action against businesses that violate the data protection law.

Instead of a private right of action, the Kentucky Attorney General will have exclusive enforcement authority. Prior to any enforcement action, the Kentucky Attorney General is required to provide the business a 30 day notice allowing the business 30 days to cure the alleged violation. It is only if the alleged violation is not cured within such 30 day period that the Kentucky Attorney General can bring an enforcement action.

Conclusion

As more 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.