CLIENT ALERTS & INSIGHTS

Indiana Becomes Seventh U.S. State to Enact an Omnibus Data Protection Law

APRIL 24, 2023

Indiana continues the 2023 trend of Midwest States enacting data protection laws under a "controller" and "processor" model. On April 13, 2023 the Indiana state legislature passed the Indiana Consumer Data Protection Law (the "Indiana Law") joining California, Colorado, Connecticut, Iowa, Utah, and Virginia in enacting broadly applicable data privacy and data security requirements on businesses.

California and Virginia's data protection laws are already in effect, with California delaying enforcement until July 2023. Colorado, Connecticut, and Utah's data protection laws will come into effect over the course of 2023 as more and more businesses in the U.S. becomes subject to one or more data protection laws. Iowa more recently passed their data protection law last month and it will go into effect January 1, 2025.

The Indiana Law provides a long runway for in-scope entities to come into compliance as the effective date of the Indiana Law is January 1, 2026. Prior to 2021, California was the only U.S. state with a comprehensive data protection law.

Now, there are 7 and 2023 will likely continue to see more states enter the data protection foray so as not to be left behind from the wave of data protection legislation. 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.

Effective Dates

State Law	Countdown	Effec
California Privacy Rights Act ("CPRA")	**In Effect**	Janua
Virginia Consumer Data Protection Act	**In Effect**	Janua
Colorado Privacy Act	**T-Minus 2 Months**	July 1
Connecticut Act Concerning Personal Data Privacy and Online Monitoring	**T-Minus 2 Months**	July 1
Utah Consumer Privacy Act	**T-Minus 8 Months**	Dece
Iowa Act Relating to Consumer Data Protection	**T-Minus 1 year and 8 months**	Janua

Indiana Consumer Data Protection Law	**T-Minus 2 years and 8 months**	Janua

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

All states set forth a prerequisite that only a business that operates or does 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 could bring a business into the scope of a U.S. state data protection law: (1) annual 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.

State	**Annual Gross Revenue (Aggregate / Worldwide)**	**Processing of Personal Information (Applicable State Residents)**	**Sale of P Resident**
California	OVER $25 million	Buying, selling, or sharing 100,000 or more consumers' personal information	50% of g personal
Colorado	N/A	Processing 100,000 or more consumers' personal information	Receiving informati consume
Virginia	N/A	Processing 100,000 or more consumers' personal information	Deriving selling pe at least 2
Connecticut	N/A	Processed 100,000 or more consumer' personal information	Deriving selling pe at least 2
Utah	**REQUIREMENT:** $25 million or more	Processing 100,000 or more consumers' personal information	Deriving selling pe at least 2
Iowa	N/A	Processing 100,000 or more consumers' personal information	Deriving selling pe at least 2
Indiana	N/A	Processing 100,000 or more consumers' personal information	Deriving selling pe at least 2

As the above table indicates, each state has taken a slightly different approach. California arguably has the broadest reach in that **any** business that records an annual gross revenue of over $25 million is subject to the CPRA.

It is also important to note a big difference between California and the other 6 U.S. states-California includes employee, job applicant, contractor, and business-to-business personal information in the scope of the law. The other 5 U.S. states all include broad exclusions that exempt out the forgoing employee and business-to-business personal information categories.

Utah is still arguably the narrowest in scope in that on top of the "do business in the state" threshold requirement, Utah also requires a prerequisite that the business have an annual gross revenue of $25 million or more. Then, assuming the first two prerequisites are met, a business must meet one of the two collection or sale of personal information triggers.

Indiana Data Protection Law Privacy Rights

The Indiana Law is most similar to Virginia's data protection law, especially in terms of data privacy rights that consumers have and the fact that a "sale" of personal information is only defined to mean the exchange of such information for money.

Under the Indiana Law, consumers will having 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 the collection and processing of their sensitive personal data; 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 new laws in Colorado, Connecticut, Iowa, Utah, and Virginia-Indiana requires businesses to give consumers the right to appeal that businesses denial of a data privacy right request.

Like Utah, the Indiana Law focuses on providing opt-out rights with regard to sensitive personal information, instead of requiring businesses to obtain prior opt-in consent such is the case under the Colorado, Connecticut, and Virginia data protection laws. The Indiana Law defines "sensitive personal data" as any category of data identifying: (1) race, ethnicity, or religion; (2) mental or physical health diagnosis; (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).

Indiana Data Protection Law Enforcement

In line with the new U.S. state data protection laws, the Indiana Law does not provide individuals with a private right of action against businesses that violate the Indiana Law.

Instead of a private right of action, the Indiana state attorney general will have exclusive enforcement authority. Prior to any enforcement action, the state 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 state attorney general can bring an enforcement action.

Conclusion

In 2022, the federal government again failed to seriously consider an omnibus data protection law that would preempt the increasing number of state data protection laws; and it is unlikely the federal government will implement such a federal law anytime soon.

Meanwhile, states will continue to enter the fray of comprehensive data protection laws. While those laws will undoubtably cover similar concepts-they will all present different and important nuances that will require detailed reviews of data protection compliance programs. This has proved true in 2021 and 2022 with California, Colorado, Connecticut, Utah, and Virginia; and now in 2023 with Iowa and Indiana.

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 require 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 difference 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.