Insights: Alerts

Are You Ready for Eight More Privacy Laws in 2025?

October 28, 2024

Written by **Meghan K. Farmer, Gregory P. Silberman, Katherine S. Kubik,**

As state-level privacy laws continue to expand in the absence of federal legislation, businesses must prepare to meet a growing patchwork of requirements or risk penalties and reputational harm. In 2025, eight additional states' comprehensive privacy laws will come into effect, further increasing the complexity of compliance. By the end of next year, approximately 150 million Americans—43% of the U.S. population—will be covered by comprehensive state-level privacy regulations. Most of the activity next year will take place in January, when five states (Iowa, Delaware, Nebraska, New Hampshire, and New Jersey) have privacy laws going into effect, with three more following later in the year.

Why This Matters

Navigating this evolving landscape of state privacy laws is critical for most companies doing business within the United States. Non-compliance could lead to regulatory penalties, legal liabilities, and loss of consumer trust. The good news is that if your business is already in compliance with existing privacy laws, only minor adjustments will likely be needed to align with the new requirements.

Key Dates by State

- Iowa – Data Privacy Law (Effective January 1, 2025)
- Delaware – Personal Data Privacy Act (Effective January 1, 2025)
- Nebraska – Data Privacy Act (Effective January 1, 2025)
- New Hampshire – Privacy Act (Effective January 1, 2025)
- New Jersey – Data Privacy Law (Effective January 15, 2025)
- Tennessee – Information Protection Act (Effective July 1, 2025)
- Minnesota – Consumer Data Privacy Act (Effective July 15, 2025)
- Maryland – Online Data Privacy Act (Effective October 1, 2025)

Determining Applicability

As companies prepare to comply with new state privacy laws, the first step is to determine whether they are subject to the regulations. Each state's privacy law applies differently depending on a company's revenue and the volume of personal data processed. Most states impose privacy obligations on any company “doing business in the state,” regardless of annual revenue. The Tennessee Information Protection Act sets an

independent revenue threshold of $25 million or more in annual revenue for a company to be covered by the law.

Except for Nebraska, most states have thresholds based on the number of residents whose personal data is processed, with lower thresholds for companies that generate significant revenue from selling personal data. Nebraska, following Texas' model, applies its law to any company that operates in the state, processes or sells personal data, and is not classified as a small business under the federal Small Business Act.

	Iowa	Delaware	Nebraska	New Hampshire	New Jersey	Tennessee	Minnesota	Maryland
Jurisdiction Threshold	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state	Doing business in the state + $25 million revenue	Doing business in the state	Doing business in the state
AND ONE OF THE FOLLOWING								
Processing Threshold	100,000+ consumers	35,000+ consumers (excluding payment transactions)	Processes or sells personal data and is not a small business	35,000+ consumers	100,000+ consumers (excluding payment transactions)	175,000+ consumers	100,000+ consumers	35,000+ consumers (excluding payment transactions)
Sale Threshold	25,000+ consumers & 50% of revenue from selling data	10,000+ consumers & 25% of revenue from selling data	None	10,000+ consumers & 25% of revenue from selling data	25,000+ consumers & any revenue or discounts from selling data	25,000+ consumers & 50% of revenue from selling data	25,000+ consumers & 25% of revenue from selling data	10,000+ consumers & 25% of revenue from selling data

As with earlier state privacy regulations, the new laws introduce variations in exemptions, including business-to-business (B2B) data, employee data, or data covered under the Gramm-Leach-Bliley Act (GLBA). After determining jurisdictional applicability, companies should carefully review available industry exemptions (the scope of which varies slightly under each law) to assess whether any exceptions apply to their operations.

As a practical matter, moreover, there are a few reasons why many companies take a single national approach to compliance and forgo analyzing whether the company meets the revenue or processing thresholds under each law. First, the laws are largely aligned, so complying with an additional state law typically requires little net new compliance work. Second, revenue and number of consumers' data processed may vary from year to year, which would create the awkward position of the law's applicability changing by year. Third, as a matter of customer service, companies may choose to comply with a consumer's request even if the state law doesn't technically apply to the company.

Obligations Across States

While each state has its own requirements, they generally align with the obligations established by earlier privacy laws. Consumers are granted the right to opt out of targeted advertising, the sale of personal data, and —except in Iowa—profiling based on personal data. Most states also require consumer opt-in for the processing of sensitive data. Iowa allows consumers to opt out of sensitive data processing, and Maryland prohibits its sale, requiring that sensitive data be processed only as necessary to provide the requested service or product. In all states, consumers have the right to access, delete, correct (except in Iowa), and obtain a copy of their personal data.

Similar to previous state privacy laws, all of the new laws will require companies to maintain a privacy notice, establish contracts with third parties who process personal data on the company's behalf, follow practices to minimize data usage, implement technical and organizational measures to protect the security of personal data, and prohibit retaliation against consumers for exercising their privacy rights. With the exception of Iowa, the new regulations also prescribe GDPR-like requirements for data protection assessments for certain use cases, such as the sale of personal data, targeted advertising, profiling, sensitive data processing, and (in Nebraska, Tennessee, and Minnesota) processing that poses a heightened risk of harm to consumers.

Unique State Obligations

While the new privacy laws are largely aligned, there are specific obligations that companies must address based on their processing activities and applicable state laws (n.b., some of these requirements are currently in force in one or more other states):

- New Jersey and Maryland require companies to stop processing a consumer's personal data within 15 and 30 days, respectively, after consent is revoked.
- Delaware, Minnesota, and Maryland grant consumers the right to request a list of third parties to whom their personal data has been disclosed.
- Minnesota allows consumers to contest profiling outcomes based on their data and mandates clear hyperlinks labeled “Your Opt-out Rights” or “Your Privacy Rights.”
- Several states, including Nebraska, Delaware (starting January 1, 2026), New Hampshire, New Jersey, Minnesota, and Maryland, require companies to honor universal opt-out mechanisms for data processing. The Texas privacy law's obligation to respond to universal opt-out mechanisms also takes effect on January 1, 2025.

Companies should decide whether to extend these rights to all consumers or restrict them to residents of the applicable states.

All Eyes on Annapolis

Of the laws taking effect in 2025, Maryland's law presents the greatest compliance and product development challenges. For example, Maryland's law limits the collection of personal data to that which is “reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains.” Moreover, the law prohibits targeted advertising to individuals younger than 18 years old and selling sensitive personal data.

Those data use restrictions could essentially end certain behavioral advertising and data brokering use cases. However, we recommend analyzing each use case against various exceptions in the Maryland law (those exceptions are available at both the processing activity and entity level).

How to Prepare

As a first step, review when your company's privacy policy was last updated and assess whether you are compliant with current privacy laws. Then, determine if the new laws will apply to your business. Ensure that you allocate enough time to update both your privacy policy and internal procedures to meet existing obligations as well as the new laws coming into effect in 2025.

Your company should also ensure that any specific obligations under these laws are clearly addressed and that all technical and operational requirements are functioning properly. Our team can assist in reviewing your privacy policy for compliance with these new regulations, and a checklist of key elements is provided at the end of this alert.

Additionally, you will need to update your data collection and processing practices to handle consumer rights requests in line with each state's rules. If you respond to consumer requests based on the individual state of residence, ensure you have processes in place to meet each state's unique requirements.

Privacy Policy Checklist

- Include categories of personal data processed.
- Specify the purpose of processing.
- Provide a method for consumers to exercise their rights.
- Disclose categories of personal data shared with third parties.
- List categories of third parties with whom data is shared.
- Include the controller's contact information.
- Include an opt-out mechanism for the sale of data, targeted advertising, and profiling (if applicable).
- Ensure compliance with specific state opt-out mechanisms (e.g., “Your Opt-out Rights” hyperlink in Minnesota and a means to request a list of specific third parties with whom a consumer's personal data has been shared for residents of Delaware, Minnesota, Oregon, and Maryland).
- Evaluate the need to implement functionality that recognizes and appropriately responds to Do Not Track signals and other opt-out mechanisms required by applicable state laws, such as the Global Privacy Control (GPC).

Related People

Meghan K. Farmer

t 404.541.6816

mfarmer@ktslaw.com

Gregory P. Silberman

t 650.462.5310

gsilberman@ktslaw.com

Katherine S. Kubik

t 404.532.6961

kkubik@ktslaw.com