POLSINELLI

Publications

February 26, 2025 • Updates

2024 State Consumer Privacy Law Year-in-Review

It was a busy year for state legislatures seeking to protect their residents' privacy. In 2024, seven states passed comprehensive consumer privacy laws: Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey and Rhode Island. At a high level, these states have not deviated greatly from their predecessors, with each:

- Obligating businesses to limit their processing of consumers' personal data to specific purposes;
- Imposing transparency obligations (e.g., providing consumers a compliant privacy notice or policy);
- Requiring businesses to recognize certain consumer rights, particularly with respect to access/portability, deletion and correction;
- Prohibiting or limiting the collection of "sensitive data" without consent;
- Requiring organizations to allow consumers to opt out of certain processing activities, such as the sales of personal data, targeted advertising and profiling or automated decision-making.

Each of these laws also exempts, with some variation, data or entities subject to the Health Insurance Accountability and Affordability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA) and other federal sectoral privacy laws.

Organizations already complying with the existing patchwork of state consumer privacy laws should be well positioned to comply with these new laws as they come into effect over the next two years. The devil, however, is in the details, and these new laws depart from existing state consumer privacy laws in novel ways. Below we summarize at a high level the fundamental aspects of these laws and some notable departures from other state consumer privacy laws, organized by each law's effective date. However, organizations that operate in these states will want to carefully analyze the new laws to identify any impact to their existing privacy compliance programs.

Nebraska — Effective Date: January 1, 2025

The Nebraska Data Privacy Act (the Nebraska Act) differs from most other state privacy laws — but aligns with Texas' consumer privacy law — in that it does not apply a

Related People

- Alexander S. Altman
- Elizabeth Snyder

Related Capabilities

- US State Privacy Laws

threshold of processing activity to determine which entities are in scope. Rather, any entity doing business in the state is subject to the Nebraska Act. Along with other common exemptions, however, the Nebraska Act generally exempts small businesses, as defined by the Small Business Administration, with the exception of restrictions on sales of sensitive data without consumer consent, which all businesses must follow.

The Nebraska Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data.

New Hampshire — Effective Date: January 1, 2025

New Hampshire Senate Bill 255 (the New Hampshire Act) adopts a structure and thresholds similar to existing state privacy laws, applying to "controllers" that do business in New Hampshire and that, during a calendar year, either (1) control or process the personal data of at least 35,000 New Hampshire consumers, or (2) control or process personal data of 10,000 New Hampshire consumers and derive over 25% of gross revenue from the sale of personal data. Unusually, the 35,000-consumer threshold excludes "personal data controlled or processed solely for the purpose of completing a payment transaction."

The New Hampshire Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data and must honor consumers' revocation of such consent.

New Jersey — Effective Date: January 15, 2025

New Jersey Senate Bill 332 (the New Jersey Act) will apply to controllers that do business in New Jersey and, during a calendar year, either (1) control or process the personal data of at least 100,000 New Jersey consumers, or (2) control or process personal data of 25,000 New Jersey consumers and derive any revenue from the sale of personal data. The New Jersey Act has no exemption for nonprofit organizations and, unlike most state consumer privacy laws, does not exempt data or entities subject to FERPA.

The New Jersey Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data and must honor consumers' revocation of such consent. The New Jersey Act is atypical — joined only by California's and Colorado's laws — in that it provides for a regulatory framework, requiring the director of the Division of Consumer Affairs in the Department of Law and Public Safety to promulgate rules necessary to further the purposes of the act. The New Jersey Act does not impose a deadline for the promulgation of rules, so it remains to be seen when and how they may impact enforcement.

Minnesota — Effective Date: July 31, 2025

The Minnesota Consumer Data Privacy Act (the Minnesota Act) will apply to controllers that do business in Minnesota and, during a calendar year, either (1) control or process the personal data of at least 100,000 unique Minnesota consumers, or (2) control or process personal data of 25,000 unique Minnesota consumers and derive over 25% of gross revenue from the sale of personal data. Notably, the Minnesota Act also largely exempts small businesses (with the exception of restrictions on sales of sensitive data

without consent). Like the New Jersey Act, the Minnesota Act does not have a blanket exemption for nonprofits. It does, however, exempt nonprofits that are established to detect and prevent insurance fraud.

The Minnesota Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data and honor consumers' revocation of such consent.

Interestingly, the Minnesota Act gives consumers the right to request the specific third parties to which a controller has disclosed the consumer's personal data. Almost all other state consumer privacy laws require only that controllers be transparent about the categories of third parties to which they have made disclosures. This could pose a substantial burden on some controllers.

Additionally, the Minnesota Act uniquely gives consumers the right to question the results of profiling. Specifically, Minnesota consumers have the right to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future. The consumer has the right to review the personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

Maryland — Effective Date: October 1, 2025

The Maryland Online Data Privacy Act (the Maryland Act) will apply to controllers that do business in Maryland and that, during the preceding calendar year, (1) controlled or processed personal data of at least 35,000 Maryland consumers, or (2) controlled or processed personal data of 10,000 Maryland consumers and derived more than 20% gross revenue from the sale of personal data. Like the Minnesota Act, the Maryland Act does not broadly exempt nonprofit entities. Rather, it exempts only nonprofits that process personal data either to assist law enforcement agencies in investigating criminal or fraudulent acts relating to insurance or to assist first responders responding to catastrophic events.

The Maryland Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. The Maryland Act imposes unique obligations surrounding sensitive data, requiring controllers to adhere strictly to data minimization requirements and prohibiting the sale of sensitive data entirely, regardless of whether a consumer provides consent.

Kentucky — Effective Date: January 1, 2026

Kentucky's Consumer Data Protection Act (the Kentucky Act) will apply to controllers that do business in Kentucky, and that, during a calendar year, either control or process the personal data of at least (1) 100,000 Kentucky consumers, or (2) 25,000 Kentucky consumers and derived over 50% of gross revenue from the sale of personal data. The Kentucky Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data.

Notably, unlike many recently enacted state privacy laws, the Kentucky Act will not require

the businesses to recognize universal opt-out mechanisms (such as Global Privacy Controls or GPCs) to process requests to opt out of sales of personal data or targeted advertising.

Rhode Island — Effective Date: January 1, 2026

The Rhode Island Data Transparency and Privacy Act (the Rhode Island Act) will apply to controllers that do business in Rhode Island and, during the preceding calendar year, either (1) controlled or processed the personal data of at least 35,000 Rhode Island consumers, or (2) controlled or processed personal data of 10,000 Rhode Island consumers and derived 20% of gross revenues from the sale of personal data.

The Rhode Island Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data and honor consumers' revocation of such consent.

While the Rhode Island Act aligns with the other state privacy laws in effectively requiring controllers to provide consumers a privacy notice or policy, it sets a high bar for transparency with respect to the sales of personal data. Unlike most of the other state consumer privacy laws, but similar to the Minnesota Act, the Rhode Island Act requires controllers to identify all third parties — not merely "categories" of third parties — to which the controller has sold or "may sell" personal data.

In sum, 2024 saw a continuation of the past several years' trend in the passage of state consumer privacy laws. While these new laws are largely similar in scope, exemptions and obligations, they do have notable differences. As effective dates approach, organizations should review these new laws and their compliance programs to ensure that any differences are accounted for.