New State Privacy Laws – Second Half of 2025

JULY 29, 2025

D. REED FREEMAN JR., ANDREA M. GUMUSHIAN, MICHELLE R. BOWLING

The state legislatures remain extremely active on privacy legislation this year. One new state comprehensive privacy law took effect on July 1, one takes effect July 31, and a third will take effect on October 1.

A total of 20 new state-level comprehensive privacy laws have been enacted since California enacted the California Consumer Privacy Act in 2018.

Some state legislatures are still in session — notably, Massachusetts, Michigan, and Wisconsin — all of which are considering new privacy legislation. Previously enacted laws are set to take effect on January 1, 2026, in **Kentucky**, **Rhode Island**, and **Indiana**. Moreover, the California Privacy Protection Agency just approved new regulations under the California Privacy Protection Act for **risk assessments, cybersecurity audits, automated decisionmaking technology, and insurance companies** and **data brokers**, while the New Jersey Attorney General has **proposed rules** under the New Jersey Data Protection Act (comment period closes on August 1).

This is a very dynamic area of law, so be sure to check this page regularly and **subscribe** to our alerts. This alert focuses on new state-level comprehensive privacy laws in **Tennessee** (effective July 1), **Minnesota** (effective July 31), and **Maryland** (effective October 1; applies to personal data processing activities beginning on April 1, 2026).

Consumers Only – Not Employees, Contractors, or B2B Data

These new laws do not apply to personal information processed or maintained in the course of employment, including information provided to a business by an individual applying to, or acting

as, an employee or in a business-to-business (B2B) context. All three of the laws' definitions of "consumer" explicitly *exclude* natural persons acting in a commercial or employment context.

(Mostly) Familiar Consumer Rights

The three laws provide consumers with rights that are largely consistent with the state privacy laws already in effect, including the right to access, delete, correct, and opt out of the sale and processing of personal data for the purposes of targeted advertising. All three states allow a consumer to appeal a business' decision to decline to take action in response to a consumer rights request.

Minnesota follows Oregon in providing consumers with the right to obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data. If the controller does not maintain the information in a format specific to the consumer, a list of specific third parties to whom the controller has disclosed any consumers' personal data may be provided instead.

Uniform Opt-Out Mechanisms – Yes for Minnesota and Maryland, No for Tennessee

Following California, Colorado, and Connecticut, Maryland and Minnesota require businesses to allow consumers to communicate their privacy preferences automatically on the business' website through the use of universal opt-out mechanisms, such as the **Global Privacy Control**. Tennessee does not currently place this obligation on covered businesses.

Minnesota and Profiling Activities

The Minnesota law contains a unique right to question the results of a business' profiling when that profiling is done in furtherance of decisions that produce legal or similarly significant effects concerning a consumer. Specifically, when a business performs that type of profiling, consumers have the right to be told the reason why such profiling resulted in a specific decision, and to be informed of actions the consumer can take to secure a different decision in the future — specifically, to review his or her personal data used in the profiling, correct inaccuracies, and have the profiling decision reevaluated based on the corrected data.

Maryland and the New Data Minimization Model

Under the Maryland law, controllers are required to limit their collection of personal data to what is reasonably necessary and proportionate to provide or maintain a *specific* product or service requested by a consumer. Controllers may not collect or process sensitive data except "where the collection or processing is *strictly necessary to provide or maintain a specific product or service requested by the consumer* to whom the personal data pertains and unless the controller obtains the consumer's consent." This is a notably stricter standard for data processing compared to other state

privacy laws, such as those in Colorado ("adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes") and California ("reasonably necessary and proportionate to achieve the purposes for which the personal information was collected" or another disclosed purpose). The Maryland standard is already serving as a model for other states' privacy legislative efforts, such as Vermont (which did not pass this year but will likely be back next year) and Massachusetts.

No New Rulemakings or Private Rights of Action

None of these state laws provides provisions for Attorney General rulemaking authority. The laws are enforced by the Attorney General in the respective state. The Attorneys General can bring a civil enforcement action against a controller or processor that violates the law. Minnesota and Tennessee specifically note a monetary penalty for violations, not to exceed $7,500 per violation under each state's law. Violations of the Maryland law can result in fines of $1,000 (first violation) or $5,000 (second and subsequent violations) per violation. None of the laws provides consumers with a private right of action.

Nonprofits Covered in Maryland and Minnesota

Notably, the Maryland and Minnesota laws *do not exempt nonprofit organizations*. These laws join a growing list of state comprehensive privacy laws (Colorado, Delaware, Maryland, Minnesota, New Jersey, and Oregon) that apply to nonprofits (at least in most cases) if the nonprofit otherwise meets the law's threshold of applicability (discussed below).

Exemptions – GLBA and HIPAA Data-Level

The Tennessee, Maryland, and Minnesota laws provide many of the same exemptions for certain types of data that we see in other state comprehensive privacy laws. All three states exempt data regulated by the Gramm-Leach-Bliley Act, data covered by the Drivers' Privacy Protection Act, data covered by the Family Educational Rights and Privacy Act, and protected health information under the Health Insurance Portability and Accountability Act (HIPAA).

Applicability Thresholds

Tennessee Information Protection Act

The Tennessee Information Protection Act applies to entities that conduct business in Tennessee or target Tennessee residents, have annual revenue exceeding $25 million, ***and*** meet one of the following thresholds:

— Control or processes the personal information of at least 175,000 consumers in Tennessee during a calendar year.

— Control or processes the personal information of at least 25,000 consumers in Tennessee and derives more than 50% of its gross annual revenue from the sale of personal information.

The thresholds are relatively high compared to some other state privacy laws, meaning the Tennessee Information Protection Act (TIPA) is targeted at larger businesses or those with significant data processing activities related to Tennessee residents.

Minnesota Consumer Data Privacy Act

The Minnesota Consumer Data Privacy Act (MCDPA) applies to entities that conduct business in Minnesota or produce products or services targeted to Minnesota residents, and that meet at least one of the following thresholds within a calendar year:

— Control or process the personal data of 100,000 or more Minnesota consumers during a calendar year, excluding personal data controlled or processed solely for the purpose of completing a payment transaction.

— Derive more than 25% of its gross revenue from the sale of personal data and process or control the personal data of 25,000 or more Minnesota consumers.

The law also applies to controllers or processors acting as "technology providers" under Minnesota law, specifically those that contract with public educational agencies or institutions to provide technology services. Small businesses, as defined by the US Small Business Administration, are generally exempt from the law, except for the requirement that they must not sell a consumer's sensitive data without the consumer's prior consent. Postsecondary institutions have an extended compliance deadline of July 31, 2029.

Maryland Online Data Privacy Act

The Maryland Online Data Privacy Act (MODPA) applies to entities that conduct business in Maryland or provide products or services targeted at residents of Maryland ***and*** during the immediately preceding calendar year:

— Controlled or processed the personal data of at least 35,000 Maryland consumers (excluding personal data controlled or processed solely for the purpose of completing a payment transaction).

— Controlled or processed the personal data of at least 10,000 Maryland consumers and derived more than 20% of its gross revenue from the sale of personal data.

The 35,000-consumer threshold is notably lower than most other state privacy laws (Connecticut and Delaware now have similar thresholds; Montana's threshold is now 25,000), making MODPA applicable to a broad range of businesses, including many small and mid-sized companies and nonprofits. MODPA does not apply to individuals acting in a commercial or employment context (it covers only Maryland residents acting in an individual or household context). The law takes effect October 1, but will not apply to personal data processing activities until April 1, 2026. This provides a six-month grace period for businesses to prepare to comply with the law.

Key Takeaways

Organizations that fall under the scope of these new privacy laws should review and prepare their privacy programs. The list of action items may involve the following:

- Data mapping and collection evaluation.
- Making updates to privacy policies.
- Implementing consumer rights request and opt-out procedures.
- Implementing the Global Privacy Control.
- Reviewing how your business is handling AdTech, marketing, and cookies on websites.
- Reviewing and updating data processing agreements with vendors.
- Considering the need to conduct risk assessments based on the data being processed.
- Reviewing data security standards.
- Providing training for employees.

If you have any questions, please reach out to your ArentFox Schiff contact or a member of the **Privacy, Data Protection & Data Security** team.

Contacts

D. Reed Freeman Jr.
PARTNER

Andrea M. Gumushian
ASSOCIATE

Michelle R. Bowling

ASSOCIATE

Related Practices

Privacy, Data Protection & Data Security

Continue Reading

PRIVACY COUNSEL

23andMe and the Role of Privacy in Bankruptcy Law

MAY 21, 2025 | D. REED FREEMAN JR., CAROLYN INDELICATO

PRIVACY COUNSEL

Nebraska Introduces First-of-its-Kind Privacy Bill Aimed at Protecting Agricultural Data

FEBRUARY 14, 2025 | D. REED FREEMAN JR., KAREN ELLIS CARR, ANDREA M. GUMUSHIAN