Westlaw Today
powered by Reuters

Recent developments in U.S. state data privacy law

By Jana Slavina Farmer, Esq., and Elisabeth Axberger, Esq., Wilson Elser

AUGUST 23, 2024

While Congress continues to work through the drafts of a comprehensive national privacy law, state legislation is continuing apace, with the 2024 state legislative session adding six more state omnibus privacy laws to the patchwork of state privacy regulation.

The new laws follow the prior models of Connecticut, Virginia and Washington laws, but feature important distinctions that are critical for organizations to be aware of in building their privacy programs. As state regulators often remind practitioners, it is the distinctions between the states' privacy laws that are frequently the focus for that state's regulators.

Rhode Island[1]

Rhode Island is the latest state to enact a data privacy law, titled the Data Transparency and Privacy Protection Act, which will take effect on January 1, 2026.

As state regulators often remind practitioners, it is the distinctions between the states' privacy laws that are frequently the focus for that state's regulators.

This law will apply to persons and entities doing business in Rhode Island that during the prior year either (1) controlled or processed the personal data of at least 35,000 Rhode Island residents or (2) controlled or processed the personal data of at least 10,000 state residents and derived more than 20% of their gross revenue from the sale of personal data.

The term "personal data" is defined in a traditional manner ("linked or reasonably linkable to an identified or identifiable individual"); de-identified and publicly available information is excluded. Notably, the law also uses the undefined term "personally identifiable information," and it is unclear if a distinction is being made from the term "personal data" (data breach notification laws, for example, narrowly define similar terms).

The law features both entity-level exemptions (nonprofits, HIPAA covered entities, financial institutions regulated by the Gramm-Leach-Bliley Act, etc. are exempted) and data-level exemptions (including employment data). As usual, because exemptions differ between states, each organization must analyze whether the law's exemptions apply to them and whether the familiar exemptions are in fact present.

The rights afforded to the Rhode Island residents largely track those available under other state laws, namely:

- The right to confirm processing
- The right to obtain a copy of personal data in readily usable format
- The right to correct inaccuracies
- The right to delete
- Opt-out rights from sale of personal data, processing for targeted advertising purposes and for profiling.

Controllers (individuals and legal entities that determine the purpose and means of processing personal data) are obligated to provide a privacy notice, implement reasonable security measures to protect the personal data, honor consumer rights requests and conduct data protection assessments when the data processing presents a heightened risk of harm to the consumer.

Processors (those who process data on controller's behalf) must adhere to controller's instructions and cooperate with the controller. Controller-processor relationships must be formalized by a contract; the law includes a list of mandatory provisions for such contracts, which are similar to the requirements of California regulations.

Notably, the law requires controllers to disclose in their privacy notice the specific third parties to which it sells or *may* sell personally identifiable information. Essentially mandating disclosure of future plans, this provision is potentially onerous. This, and the missing definition of "personally identifiable information" may require future legislative clarification.

At the same time, some of the expected provisions of other data privacy laws, such as the data minimization principle, opt-out link or universal opt-out mechanism requirements, are not included. Rhode Island law does *not* have a cure period for controllers to remedy violations.

Minnesota[2]

Minnesota's Consumer Data Privacy Act will become effective on July 31, 2025.

It will apply to controllers conducting business in, or producing products or services targeted to the residents of Minnesota, who, within a calendar year, either (1) control or process the personal data of at least 100,000 Minnesota consumers or (2) control or process personal data of 25,000 Minnesota consumers and derive 25% of gross revenue from the sale of personal data. "Personal data" is defined in the same manner as in Rhode Island.

On the entity level, Minnesota's law exempts small businesses, chartered banks, credit unions and insurance companies, among others. Nonprofit organizations that are established to detect and prevent insurance fraud also are exempted.

In addition, the law features data-level exemptions, including for employment and benefits data. Notably, HIPAA-covered entities are not exempted but there is an exemption for protected health information and other categories of health-related information.

Several of the incoming state privacy laws added novel requirements to organizations' privacy compliance obligations, mandating further disclosures and maintenance of additional records, and offering different definitions that may result in altered obligations.

Consumer rights are similar to the ones discussed above for Rhode Island, with two notable additions. Minnesota follows the example of the Oregon law in giving consumers a right to obtain a list of the specific third parties to which the controller has disclosed the consumers' personal data.

Furthermore, the consumer has a right to question the result of a profiling decision that produces legal effects concerning a consumer or similarly significant effects concerning a consumer.

Minnesota's privacy policy requirements track those found in California's and Colorado's privacy regulations. A separate Minnesota-specific privacy policy is not needed. But, Minnesota will have the first U.S. law to require controllers to maintain a data inventory as well as documentation of policies and procedures adopted to comply with the Minnesota law.

Minnesota law features a 30-day right to cure violations, sunsetting on January 31, 2026.

Maryland[3]

Maryland's Online Data Privacy Act will take effect on October 1, 2025.

The thresholds of applicability consist of doing business in the state and during the prior calendar year, (1) controlling or processing personal data of at least 35,000 Maryland consumers or (2) controlling or processing the personal data of at least 10,000 Maryland consumers and deriving more than 20% of gross revenue from the sale of personal data.

The entity-level exemptions are more limited than under other state laws. For example, most nonprofits and HIPAA entities are not exempted, although there are exemptions for protected health information under HIPAA.

The Maryland law imposes novel data minimization requirements, requiring controllers to limit data collection to what is reasonably necessary and proportionate (and for sensitive data, strictly necessary) to provide or maintain a *specific* product or service requested by the consumer to whom the data pertains.

If a controller desires to process personal data for a purpose that is neither reasonably necessary to, nor compatible with, the disclosed purposes, it may only do so with consumers' consent. Sale of sensitive data or data of consumers under the age of 18 is prohibited. Notably, the wording of the statute implies that companies cannot blindly rely on lack of knowledge that a consumer is under 18, suggesting that an age verification may be necessary under some circumstances.

Entities within the scope of Maryland's law will need to take a careful look at the definitions and wordings employed by the statute. For example, biometric data is defined as "data generated by automatic measurements of the biological characteristics of a consumer that *can be used* to uniquely authenticate a consumer's identity."

Other state laws' definitions generally require that biometric identifiers be used, and not just be capable of being used, to identify an individual. Maryland also uses the term "authenticate" as opposed to "identify," but it is not clear that the statute intends a different meaning.

That said, the term "authenticate" is defined in the statute, but solely in connection with verification of consumer identity for the purposes of consumer privacy requests. It appears likely that the meaning of these and other terms of the Maryland statute will need to be clarified on a case-by-case basis, as no rulemaking is contemplated to clarify this statute.

The Maryland Division of Consumer Protection, however, has a rule-making power to further define unfair and deceptive trade practices.

New Hampshire[4]

New Hampshire's Privacy Act will go into effect on January 1, 2025, and would apply to persons that, during a one-year period, either (1) control or process personal data of more than 35,000 state consumers or (2) control or process the data of more than 10,000 state consumers and derive more than 25% of gross revenue from the sale of personal data.

This law largely tracks Connecticut's law. Notably, unlike in Connecticut, rulemaking is contemplated by the Secretary of State, who shall establish privacy notice standards and reliable means for consumers to exercise their privacy rights. A 60-day cure period for violations may be available if the Attorney General determines that a cure is possible. This provision sunsets on December 31, 2025.

Kentucky[5]

Kentucky's Consumer Data Protection Act will take effect on January 1, 2026, and will apply to controllers that either (1) control or process personal data of at least 100,000 Kentucky consumers or (2) control or process personal data of at least 25,000 Kentucky consumers and derive more than 50% of gross revenue from the sale of personal data.

The Kentucky law's provisions are less demanding on covered businesses than some other laws enacted this year, as evidenced by a more limited definition of what constitutes a sale of personal information, and lack of requirement to recognize opt-out preference signals, a provision that has otherwise become standard in recent privacy laws.

Like New Hampshire, Kentucky's statute also largely follows the lead of another state in the region, tracking Virginia's data privacy law's model but featuring several additional exemptions. The law features a 30-day permanent, nondiscretionary cure period for alleged violations.

Nebraska[6]

Nebraska's Data Privacy Act will take effect on January 1, 2025. Resembling Texas's data privacy law, the law features three cumulative criteria of applicability and will apply to persons that (1) conduct business in Nebraska or produce a product or service consumed by Nebraska residents, (2) process or sell personal data and (3) are not a small business as defined by federal law. This definition significantly broadens its applicability.

Notably, small businesses are prohibited from selling sensitive data without consumer consent. Controller obligations are to a great extent comparable to existing state laws. A 30-day right to cure violations does not sunset.

Vermont bill vetoed[7]

On May 10, 2024, the Vermont Legislature passed a comprehensive data privacy law, which was slated to become one of the country's more rigorous frameworks. However, on June 13, 2024, Governor Phil Scott vetoed the bill, outlining his concerns in a press release of the same date. First among Governor Scott's concerns is the bill's private right of action, which would have made the bill "more hostile than any other state to many businesses and nonprofits."

Governor Scott also noted that the age-appropriate design code provisions are similar to the legislation in California that has already been stopped by the courts for likely First Amendment violations, and that Vermont should await the final decision in California before charging ahead with policy that may lead to expensive lawsuits.

Finally, Governor Scott criticized the bill for creating "big and expensive new burdens and competitive disadvantages" for Vermont's businesses. Instead, Governor Scott advocates for Vermont to adopt Connecticut's version of the law, similar to what New Hampshire has done, which will promote regional consistency and benefit both the consumers and the economy.

Conclusion

Several of the incoming state privacy laws added novel requirements to organizations' privacy compliance obligations, mandating further disclosures and maintenance of additional records, and offering different definitions that may result in altered obligations.

At a more general level, a shift in the privacy landscape emerges from the earlier "notice and choice" model to a more restrictive "purpose limitation" approach to date processing, more aligned with the EU's General Data Protection Regulation and the proposed federal American Privacy Rights Act.

Adopting the "most rigorous requirements" compliance model remains a good strategy to comply with new state frameworks, but the unique provisions of these laws will nonetheless require a careful review by businesses.

Significantly, none of the new laws contains a private right of action (besides the vetoed Vermont law). However, the regulatory penalties for violations may be significant as regulators across the states interpret the statutory penalties as awardable on a per-person, per-day basis.

Notes:

[1] https://bit.ly/3LYyccO

[2] https://bit.ly/4dhs6jU

[3] https://bit.ly/46HfY9o

[4] https://bit.ly/4dwQA8d

[5] https://bit.ly/3LYl8nU

[6] https://bit.ly/3WTynMF

[7] https://bit.ly/4db80HV

About the authors

Jana Slavina Farmer, CIPP/US, is a partner with **Wilson Elser**. She is one of the leaders of the firm's consumer privacy practice and a member of the firm's intellectual property and technology practice. Farmer advises clients on data privacy compliance and emerging legal issues in the technology space, including those involving internet law, non-fungible tokens and artificial intelligence. She can be reached at jana.farmer@wilsonelser.com. **Elisabeth Axberger** (not pictured) is an associate with the firm and a member of its cybersecurity and data privacy practice and intellectual property and technology practice. Axberger represents clients in cybersecurity incidents, advising on legal obligations under breach notification laws. She also advises clients on a wide range of data privacy compliance matters under U.S. and international data privacy law. She can be reached at elisabeth.axberger@wilsonelser.com. Both authors work in the firm's New York offices.

This article was first published on Westlaw Today on August 23, 2024.