HINSHAW

Alerts

Strategic Privacy Planning Alert: A State Law Regulatory Roadmap for 2024-2025 Compliance

September 25, 2024
Privacy, Cyber & AI Decoded

As January 2025 privacy strategy planning ramps up this fall, our Privacy, Security, & Artificial Intelligence team has put together a planning alert for 2024–2025. In this installment, we review the following nine state privacy laws set to take effect soon:

1. **Montana Consumer Data Privacy Act** (October 1, 2024)
2. **Delaware Personal Data Privacy Act** (January 1, 2025)
3. **Iowa Consumer Data Protection Act** (January 1, 2025)
4. **Nebraska Data Privacy Act** (January 1, 2025)
5. **New Hampshire Privacy Act** (January 1, 2025)
6. **New Jersey Data Protection Act** (January 15, 2025)
7. **Minnesota Consumer Data Privacy Act** (July 31, 2025)
8. **Tennessee Information Protection Act** (July 1, 2025)
9. **Maryland Online Data Protection Act** (October 1, 2025)

What Should Businesses Plan For?

- **Determine which laws and regulations apply to your business**, as these nine upcoming privacy laws have varying applicable thresholds and exemptions.
- **Review and update consumer-facing privacy policies** to include consumer rights under the applicable laws for compliance and to ensure that these privacy notices are simple and accurate regarding your current privacy practices. In **some** states, consumer rights include the right to "opt-in" for using sensitive personal data.
- **Assess and update your risk and contractual processes**, including implementing data privacy impact assessments and data protection agreements for service providers/processors and third parties. Regulators can and will ask for these documents. Ensure your data team is considering data minimization and has the applicable regulatory controls in place for aggregated and de-idenfified data.
- **Adopt and implement reasonable administrative, technical, and physical practices for personal data security.** Be aware that there is now an additional state regulatory cause of action if your security does not meet these standards and there is a data breach.

Attorneys

Sabrina Janeiro

Cathy Mulrow-Peattie

Jason J. Oliveri

J. Michael Paulino

Service Areas

Privacy, Security & Artificial Intelligence

- **Understand that while none of these states have a private right of action, we expect all states to begin enforcing these laws**, with many states growing their privacy enforcement staffs. Although there is a right to cure in some of these states, that right varies by state and, as always, by regulator.

Keep reading to review some of the unique aspects of these nine laws and assess whether they apply to your business.

1. Montana Consumer Data Privacy Act (MOCDPA)

Effective October 1, 2024

- As for processing sensitive data, the MOCDPA requires obtaining the consumer's prior consent only. Sensitive data is defined in the MOCDPA in a limited way as a person's racial or ethnic origin, religious beliefs, mental or physical condition or diagnosis, information about a person's sex life, sexual orientation, citizenship or immigration status, the processing of genetic or biometric data for the purposes of uniquely identifying the individual and precise geolocation data.
- The Montana Attorney General is relegated to enforcing the MOCDPA, and there is a 60-day cure period.

2. Delaware Personal Data Privacy Act (DPDPA)

Effective January 1, 2025

The DPDPA imposes obligations upon controllers and processors, including to:

- limit the collection of personal data that is reasonably necessary for the disclosed purposes;
- maintain data security measures to protect consumer data; and
- process sensitive data only after obtaining the consumer's consent.

3. Iowa Consumer Data Protection Act (ICDPA)

Effective January 1, 2025

The ICDPA imposes varying obligations, including that it:

- does **not** require that consumers opt-in for the processing of "sensitive data," nor does it grant the right to correct or opt out of profiling; and
- requires that controllers/businesses have a data processing agreement in place with ICDPA-specific terms.

The ICDPA also has a 90-day cure period for enforcement actions.

4. Nebraska Data Privacy Act (NDPA)

Effective January 1, 2025

The NDPA requires data protection assessments for a broad range of processing activities, such as:

- the processing of personal data for purposes of targeted advertising;
- the sale of personal data;
- the processing of personal data for purposes of profiling when the profiling presents a reasonably foreseeable risk of:

    (i) unfair or deceptive treatment of or unlawful disparate impact on any consumer;

    (ii) financial, physical, or reputational injury to any consumer;

(iii) a physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of any consumer, if the intrusion would be offensive to a reasonable person; or

(iv) other substantial injury to any consumer;

- the processing of sensitive data; and
- any processing activity that involves personal data that presents a heightened risk of harm to any consumer.

As with other comprehensive state privacy laws, controllers/businesses shall make a data protection assessment available to the Nebraska Attorney General pursuant to a civil investigative demand.

5. New Hampshire Privacy Act (NHPA)

Effective January 1, 2025

The NHPA is a more moderate comprehensive privacy law and contains the following similar requirements for controllers/businesses to help:

- Limit the collection of personal data to only what is adequate, relevant, and reasonably necessary to accomplish the purposes for which the data is processed and implement privacy by design principles.
- Implement and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.
- Provide an effective means to revoke consent that is at least as easy as the mechanism by which the consumer provided consent and which, if exercised, should cause the controller to cease processing within 15 days after receipt of the request.

6. New Jersey Data Protection Act (NJDPA)

Effective January 15, 2025

- The NJDPA also requires risk assessments under circumstances when consumer risk is heightened. These assessments should identify and weigh the benefits that may flow, directly or indirectly, from the planned data processing activity, the potential risks caused by the activity, and any mitigation safeguards that may be employed to reduce such risks.
- Businesses should note that they must provide these assessments to the New Jersey Attorney General Division of Consumer Affairs in the Department of Law and Public Safety upon request. Please note as well that this office has expanded its enforcement staff.

7. Minnesota Consumer Data Privacy Act (MCDPA)

Effective July 31, 2025

- The MCDPA requires processors and controllers to have contractual agreements regarding the processing (collection, use, disclosure, deletion, and storage) of personal data.
- This contract must contain specific processing instructions and limitations on the use of the personal information, an enumerated list of the personal information exchanged under the agreement, the rights and obligations of the parties, the duration of the processing, a duty of confidentiality, security controls, terms governing sub-processors and a right to audit.

8. Tennessee Information Protection Act (TIPA)

Effective July 1, 2025

- The TIPA, similar to other state privacy laws, does not require businesses/controllers to delete information that it maintains or uses as aggregate or de-identified data, provided that such data in the possession of the business is not linked to a specific consumer.
- The TIPA contains specific requirements for the de-identification of data, including that the controller/business in possession of de-identified data shall:

  (i) take reasonable measures to ensure that the data cannot be associated with a natural person;

  (ii) publicly commit to maintaining and using de-identified data without attempting to reidentify the data; and

  (iii) contractually obligate recipients of the de-identified data to comply with this part.

9. Maryland Online Data Protection Act (MODPA)

Effective October 1, 2025

- The heightened data minimization requirements deviate the MODPA from those terms found in some state privacy laws. Businesses/controllers are limited to collecting personal data that is "reasonably necessary and proportionate to provide or maintain a product or service requested by the consumer to whom the data pertains."
- Also, under the MODPA, collecting, processing, or sharing "Sensitive Data" is prohibited unless the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer.
  - Sensitive Data is defined broadly as personal data revealing racial or ethnic origin; religious beliefs; physical or mental health status, including gender-affirming treatments and reproductive or sexual health care; sex life or sexual orientation; status as transgender or non-binary; national origin; citizenship or immigration status; genetic or biometric data; data collected from a known child; and precise geolocation data.

Stay tuned for our next installment on cybersecurity regulations planning for 2025 by subscribing to our *Privacy, Cyber, & AI Decoded* alerts here and our upcoming Hinshaw Privacy, Cyber, and AI Decoded Virtual Roundtable.