

Insights: Alerts

Five New State Privacy Laws Effective January 2025

December 17, 2024

Written by John M. Brigagliano, Tatum Andres

Starting January 2025, five state privacy laws will take effect, providing consumer privacy rights to a new swath of individuals across the country. Delaware, Iowa, Nebraska, and New Hampshire's laws will go into effect on January 1, 2025, while New Jersey's law will follow on January 15, 2025. Below, we provide an overview of these laws, highlight key distinctions, and outline shared compliance requirements for businesses.

January will also see changes to existing privacy laws, like Texas's, which will require businesses to respond to universal opt-out mechanisms (e.g., the Global Privacy Control) as a means for consumers to opt out of targeted advertising. Businesses should double check compliance with this requirement given that Texas's law is so actively enforced.

However, some of the most significant changes to the privacy landscape will emerge later in 2025. Maryland and Minnesota's comprehensive privacy laws will spawn material new compliance requirements. Colorado's updated law will add new obligations related to biometrics and children's data, while New York's legislation on online safety for children and teens will also come into force.

Finally, California regulators are expected to finalize groundbreaking AI and privacy regulations next year. For more details, check out our latest [alert](#) on that upcoming development.

Stay tuned for further updates to help your business navigate this evolving regulatory environment!

Overview of New State Privacy Laws

Delaware Personal Data Privacy Act (DPDPA)

- **Effective Date:** January 1, 2025
- **Applicability:** Covers entities doing business in Delaware or targeting its residents, meeting specific thresholds:
 - Processes personal data of 35,000 or more consumers (excluding data solely for payment transactions),¹ or
 - Processes personal data of 10,000 or more consumers with over 20% revenue from its sale.²
- **Penalties:** Up to \$10,000 per violation; 60-day cure period ends January 1, 2026.³

Iowa Consumer Data Protection Act (ICDPA)

- **Effective Date:** January 1, 2025

- **Applicability:** Targets entities doing business in Iowa or directing services/products to its residents, meeting thresholds:
 - Processes personal data of 100,000 or more consumers,⁴ or
 - Processes personal data of 25,000 or more consumers and derives over 50% of revenue from selling personal data.⁵
- **Penalties:** Up to \$7,500 per violation; non-sunsetting 90-day cure period.⁶

Nebraska Data Privacy Act (NDPA)

- **Effective Date:** January 1, 2025
- **Applicability:** Applies to entities doing business in Nebraska or targeting its residents, meeting specific thresholds:
 - Processes personal data or engages in the sale of personal data; and does not qualify as a small business under the federal Small Business Act.⁷
- **Penalties:** Up to \$7,500 per violation; non-sunsetting 30-day cure period.⁸

New Hampshire Data Privacy Act (NHDPDA)

- **Effective Date:** January 1, 2025
- **Applicability:** Includes businesses operating in New Hampshire or targeting its residents, meeting thresholds:
 - Processes personal data of 35,000 or more consumers (excluding payment-related data),⁹ or
 - Processes personal data of 10,000 or more consumers and derives over 25% of revenue from its sale of personal data.¹⁰
- **Penalties:** Up to \$10,000 per violation; 60-day cure period ends January 1, 2026.¹¹

New Jersey Data Privacy Act (NJDPDA)

- **Effective Date:** January 15, 2025
- **Applicability:** Covers entities doing business in New Jersey or targeting its residents, meeting specific thresholds:
 - Processes personal data of 100,000 or more consumers (excluding payment-related data),¹² or
 - Processes personal data of 25,000 or more consumers with revenue tied to its sale.¹³
- **Penalties:** Up to \$10,000 for first violations; \$20,000 for subsequent violations; 30-day cure period ends July 15, 2026.¹⁴

Notable Distinctions

Delaware's privacy law is notable for its application to nonprofit organizations and educational institutions, which are typically exempt from other state privacy laws. The law also stands out for explicitly including pregnancy status and nonbinary identity within its definition of 'sensitive data.' Similarly, New Jersey's law expands the definition of 'sensitive data,' but it does so by incorporating financial credentials such as account numbers, login details, and PINs. Nebraska's law, on the other hand, is distinctive for exempting small businesses, thereby narrowing its scope compared to other state privacy laws. However, it adopts a broad definition of 'sale,' akin to California and Connecticut, which includes the exchange of personal data for monetary or other valuable

consideration. Notably, under California law, this broad definition means that a company paying another party can also 'sell' data to that party with the consideration taking the form of services or price discounts.

Shared Obligations Across States

Despite their differences, these new laws generally align with established privacy frameworks. Consumers have the right to opt out of targeted advertising, the sale of personal data, and profiling with a legally significant effects based on personal data (except in Iowa). Most states require opt-in consent for processing sensitive data, although Iowa and Utah allow opt-out consent (and many use cases for sensitive data fall under exceptions to the consumer privacy laws). All states provide consumers with the rights to access, delete, and obtain copies of their personal data, and most allow corrections, with Iowa as an exception.

Businesses are also required to maintain privacy notices, establish contracts with third-party processors, minimize data usage, implement robust security measures, and avoid penalizing consumers for exercising their rights. Most states with comprehensive privacy laws mandate GDPR-like data protection assessments for high-risk activities, including data sales, targeted advertising, profiling, and sensitive data processing. Nebraska's law also requires assessments for activities that pose a significant risk of harm to consumers, while Iowa does not include these requirements.

Key Takeaways for Businesses

We foreshadowed that the privacy landscape will continue to evolve throughout 2025. Maryland's law will introduce stronger consumer protections by prohibiting the sale of sensitive data and restricting its processing to strictly necessary purposes. Similarly, Minnesota's privacy law (i) notably does not contain an entity-level GLBA exception and (ii) will require each controller to maintain a detailed data processing inventory.

To prepare for compliance, businesses should assess whether these laws apply to their operations, update privacy notices and consumer rights management processes. For additional guidance, be sure to visit our blog regularly for the latest updates and insights.

¹ DPDPA § 12D-103(a)(1).

² DPDPA § 12D-103(a)(2).

³ DPDPA § 12D-111(b).

⁴ ICDPA § 715D.2 (1)(a).

⁵ ICDPA § 715D.2 (1)(b).

⁶ ICDPA § 715D.8(2).

⁷ NDPA § 3(1).

⁸ NDPA § 22.

⁹ NHDPA § 507-H:2(a).

¹⁰ NHDPA § 507-H:2(b).

¹¹ NHDPA § 507-H:11.

¹² NJDPA § 2(a).

¹³ NJDPA § 2(b).

¹⁴ NJDPA § 8.

Related People



John M. Brigagliano

t 404.815.6135

jbrigagliano@ktslaw.com



Tatum Andres

t 312.628.7183

tandres@ktslaw.com