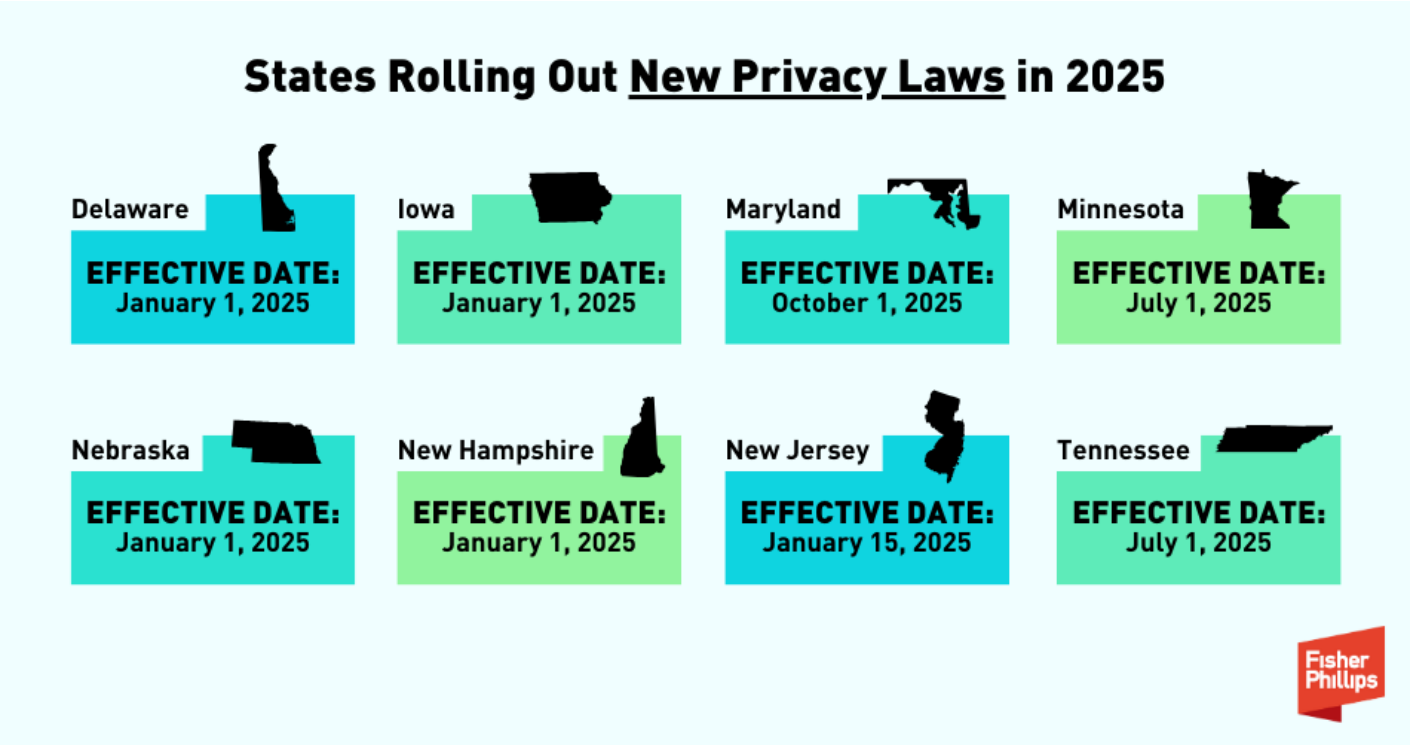
2025 State Privacy Laws Taking Effect: Key Compliance Considerations for Employers and Businesses

Insights
3.17.25

With eight states rolling out new privacy laws in 2025 and many more already on the books, businesses have never faced a more fragmented regulatory landscape. These laws will expand consumer rights, impose stricter data governance obligations, and create a complex compliance environment for businesses operating across state lines. While these laws share common frameworks, key differences – particularly Maryland's stringent requirements – will require you to take a strategic approach. Below, we break down each law's unique requirements and provide practical guidance you can put into place right away.



Delaware Personal Data Privacy Act (DPDPA)

Effective Date: January 1, 2025

Who is Covered: Businesses that control or process personal data of at least 35,000 Delaware residents, or 10,000 residents if 20% of gross revenue comes from selling personal data.

Key Requirements:

Key Requirements:

- **Universal Opt-Out:** Requires businesses to implement universal opt-out mechanisms (e.g., Global Privacy Control) by January 1, 2026.
- **Third-Party Disclosures:** Mandates disclosure of third-party data recipients in response to access requests
- **Nonprofit Inclusion:** Applies to nonprofits and educational institutions.
- **Data Protection Assessments:** Conduct assessments for high-risk processing activities.
- **60-day cure period** until December 31, 2025; then AG's discretion.

You can read more about Delaware's law here.

Iowa Consumer Data Protection Act (ICDPA)

Effective Date: January 1, 2025

Who is Covered: Businesses that control or process personal data of at least 100,000 Iowa consumers, or 25,000 consumers if 50% of gross revenue comes from selling personal data.

Key Requirements:

- **Limited Consumer Rights:** Unlike most states, consumers do not have the right to correct data. The law focuses primarily on the right to access and delete data.
- **Opt-Out Rights:** Mandates opt out option for data sales. However, consumers do not have the right to opt out of targeted advertising and profiling.
- **90-day cure period** with no sunset.

You can read more about Iowa's law here.

Maryland Online Data Privacy Act (MODPA)

Effective Date: October 1, 2025

Who is Covered: Businesses that control or process personal data of at least 35,000 Maryland residents, or 10,000 residents if 20% of gross revenue comes from selling personal data.

Key Requirements:

- **Youth Ad Ban:** Prohibits targeted advertising to individuals under 18.
- **Proportionality Rule:** Data collection is limited to what's "reasonably necessary and proportionate" for services requested.
- **AI Accountability:** Requires risk assessments for AI/ML systems impacting privacy.

- **Geofencing Ban:** Prohibits tracking within 1,750 feet of healthcare facilities.
- **60-day cure** period until April 1, 2027.

You can read a full summary of Maryland's new law here.

Minnesota Consumer Data Privacy Act (MCDPA)

Effective Date: July 31, 2025

Who is Covered: Businesses that control or process personal data of at least 100,000 Minnesota residents, or 25,000 residents if 25% of gross revenue comes from selling personal data.

Key Requirements:

- **Data Inventory:** Maintain an inventory of personal data.
- **Universal Opt-Out:**Mandates a universal opt-out mechanism for data sales and targeted advertising.
- **Data Protection Assessments:** Conduct assessments for high-risk processing activities.
- **30-day cure** period until January 31, 2026.

Nebraska Data Privacy Act (NDPA)

Effective Date: January 1, 2025

Who is Covered: Applies broadly to businesses processing personal data of Nebraska residents, with exceptions for small businesses as defined by the Small Business Act.

Key Requirements:

- **Universal Opt-Out:** Mandates a universal opt-out mechanism for data sales and targeted advertising.
- **Opt-In Consent:** Mandates consumers opt-in to share sensitive data (racial/ethnic origin, health, biometrics, etc.).
- **Dark Pattern Prohibition:** Prohibits deceptive practices to manipulate users into providing personal data.
- **Risk Assessments:** Requires assessments for high-risk processing activities.
- **30-day cure** period with no sunset

New Hampshire Privacy Act (NHPA)

Effective Date: January 1, 2025

Who is Covered: Businesses that control or process personal data of at least 100,000 New Hampshire residents, or 25,000 residents if 25% of gross revenue comes from selling personal data.

Key Requirements:

- **Broad Applicability:** Applies to a wider range of businesses due to lack of revenue threshold.
- **Nonprofit Exemption:** Exempts nonprofits from its provisions.
- **Universal Opt-Out:** Mandates a universal opt-out mechanism for data sales and targeted advertising.
- **60-day cure** period until December 31, 2025; then AG's discretion.

New Jersey Data Privacy Act (NJDPA)

Effective Date: January 15, 2025

Who is Covered: Businesses that control or process personal data of at least 100,000 New Jersey residents, or 25,000 residents if any revenue comes from selling personal data.

Key Requirements:

- **Broad Definition of Sensitive Data:** Includes financial information in its definition.
- **Rapid Consent Withdrawal:** Must cease processing personal data within 15 days of consent withdrawal.
- **Universal Opt-Out:** Mandates a universal opt-out mechanism for targeted advertising and profiling.
- **30-day cure** period until July 15, 2026.

You can read more about New Jersey's law here.

Tennessee Information Protection Act (TIPA)

Effective Date: July 1, 2025

Who is Covered: For-profit businesses with annual revenue of at least $25 million that control or process personal data of at least 175,000 Tennessee residents, or 25,000 residents if 50% of gross revenue comes from selling personal data.

Key Requirements:

- **Universal Opt-Out:**Implement a universal opt-out mechanism for data sales and targeted advertising by January 1, 2026.
- **Privacy Notices:**Publish transparent privacy policies outlining data processing purposes and consumer rights.
- **Data Protection Assessments:**Conduct assessments for high-risk processing activities.
- **Sensitive Data Processing:** Requires opt-in to process sensitive data.
- **Data Minimization:**Limit collection and processing to what is necessary for intended purposes.
- **60-day cure** period with no sunset.

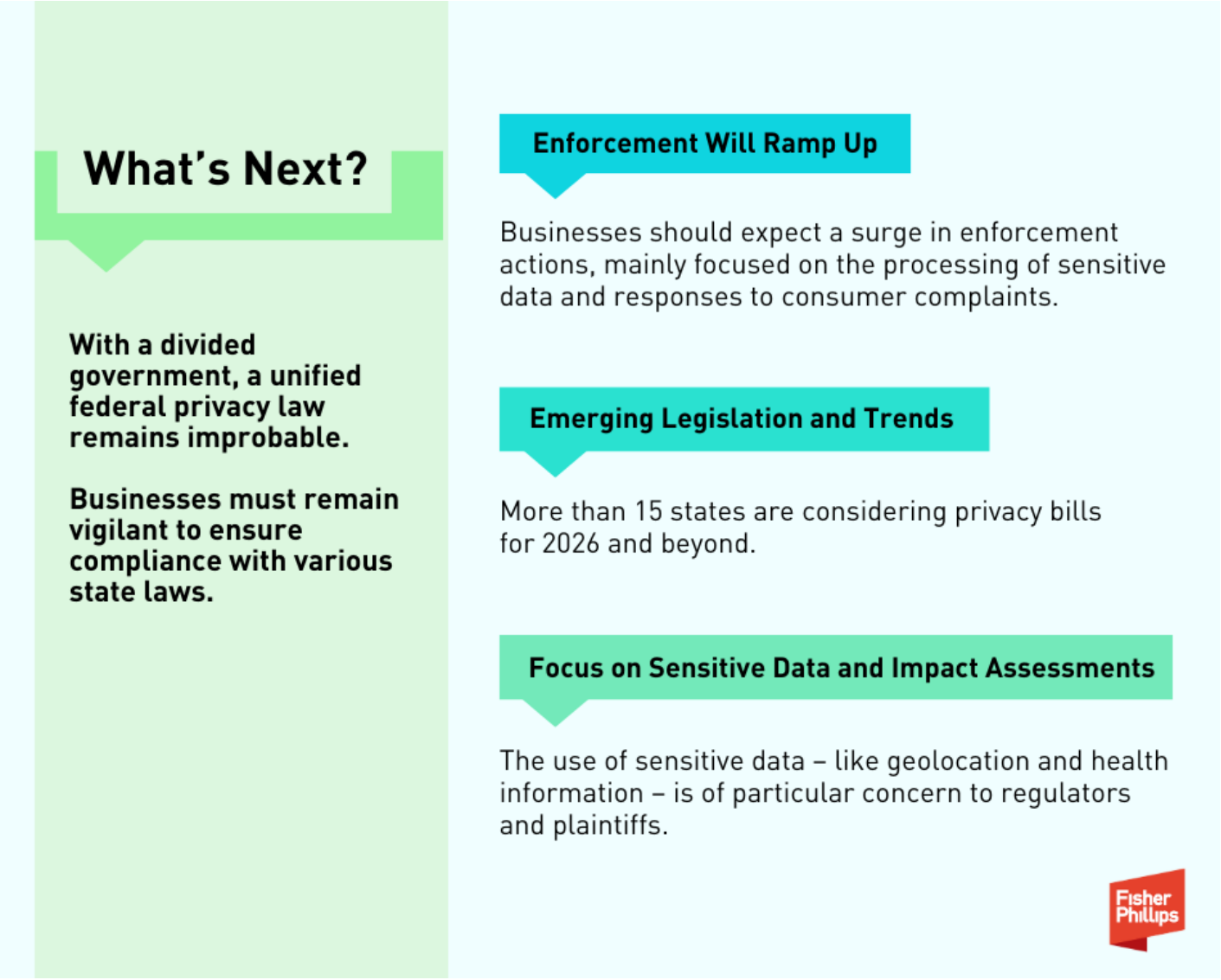
You can read more about Tennessee's law here.

The Good News

While the new state privacy laws introduce additional compliance requirements, there's a bright spot for businesses that are up to speed on their compliance obligations. Organizations that have already invested in robust privacy programs to meet existing regulations (such as CCPA or GDPR) may find themselves well-positioned. These companies will likely need only incremental adjustments to align with the new state laws, rather than wholesale changes.

What's Next?

With a divided government, a unified federal privacy law remains improbable. This prolonged legislative gridlock at the federal level will mean that the state-by-state patchwork approach to privacy regulation will remain in place for the foreseeable future. Therefore, businesses must remain vigilant to ensure compliance with various state laws.



Enforcement Will Ramp Up

2025 is poised to be a landmark year for privacy law enforcement. States are increasingly prioritizing privacy enforcement, with many new laws coming into full effect. Delaware and New Jersey, for instance, offer limited cure periods before penalties apply, signaling a more aggressive approach to enforcement. The California Privacy Protection Agency (CPPA) has already initiated investigative "sweeps" in various industries, and other states are likely to follow suit. Businesses should expect a surge in enforcement actions, mainly focused on the processing of sensitive data and responses to consumer complaints.

Emerging Legislation and Trends

More than 15 states are considering privacy bills for 2026 and beyond, indicating that privacy legislation shows no sign of slowing down. Maryland's Online Data Privacy Act (MODPA) is emerging as a potential model for future legislation, introducing stricter standards for data minimization and enhanced protections for minors. Emerging legislation increasingly focuses on AI accountability, biometric data protection, and expanded definitions of sensitive information. Meanwhile, states like

biometric data protection, and expanded definitions of sensitive information. Meanwhile, states like Massachusetts are proposing novel approaches, such as mandating Location Privacy Policies for entities collecting geolocation data. This ongoing legislative activity suggests that businesses should prepare for an increasingly nuanced and potentially more stringent privacy regulatory environment in the years to come.

Focus on Sensitive Data and Impact Assessments

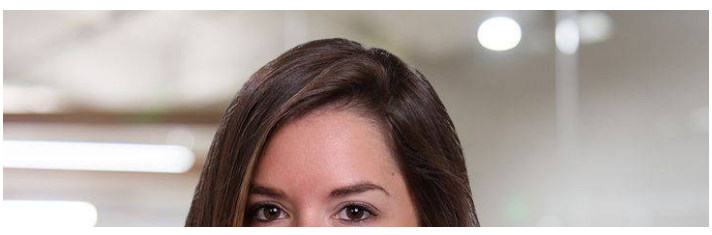
Regulators and plaintiffs are prioritizing the collection, use, and sharing of sensitive data types, especially geolocation and health information. Additionally, Data Protection Impact Assessments (DPIAs) are becoming more critical, with regulators now actively requesting these for high-risk data processing activities like targeted advertising.

Conclusion

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team. Fisher Phillips will continue to monitor any obligations and enforcement efforts and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox.

Related People

Danielle Kays
Partner
312.260.4751
Email



Monica Snyder Perl
Partner
617.532.9327
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber

Trending

U.S. Privacy Hub

Related Offices

Minneapolis

Memphis

Nashville

New Jersey

Washington, D.C.