PUBLICATION

Privacy Laws Ring in the New Year: State Requirements Expand Across the U.S. in 2026

Authors: Madison J. McMahan, Matthew George White, Alexander Frank Koskey, III
January 28, 2026

Observed annually on January 28, Data Privacy Day raises awareness about privacy and data protection.
As 2026 begins, the U.S. privacy compliance landscape reaches a pivotal moment: three new state comprehensive privacy laws take effect, and five existing statutes undergo significant amendments to eliminate cure periods or lower applicability thresholds – potentially bringing thousands of additional businesses into their scope. For organizations already managing multistate privacy obligations, this expansion represents a continuing challenge.

While Indiana, Kentucky, and Rhode Island largely follow familiar frameworks, notable changes in states such as Connecticut (dropping thresholds from 100,000 to 35,000 consumers) and Colorado (eliminating its cure period entirely) signal that compliance requirements are becoming stricter and more expensive to ignore. The good news: businesses with existing privacy programs are well-positioned to adapt, but proactive assessment and updates are essential to avoid enforcement risk in this rapidly evolving regulatory environment.

This alert provides a comprehensive overview of the three new state privacy laws taking effect in 2026 (Indiana, Kentucky, and Rhode Island) and highlights critical amendments in California, Colorado, Connecticut, Oregon, and Utah. Understanding these changes is essential for businesses to accurately assess their compliance obligations, identify new requirements, and implement necessary program updates to ensure compliance.

The Three New Comprehensive State Privacy Laws

As of January 1, 2026, Indiana, Kentucky, and Rhode Island join the growing number of states with comprehensive privacy legislation. Many of the provisions mirror frameworks that should already be familiar to businesses operating under Virginia's Consumer Data Protection Act and similar statutes, meaning the three newcomers may not introduce significant new compliance challenges for organizations already complying with state privacy laws. However, businesses should not assume complete uniformity; each state includes unique thresholds, definitions, and specific requirements that demand careful review to ensure full compliance.

Indiana Consumer Data Protection Act (ICDPA)

Indiana's new privacy law applies to entities that either:

- Control or process personal data of 100,000 or more Indiana consumers, or
- Derive 50 percent or more of gross revenue from selling personal data of 25,000 or more consumers.

Key provisions include data protection impact assessment requirements, obligations for processing deidentified or pseudonymous data, opt-in consent for processing sensitive data, consumer opt-out rights for targeted advertising and data sales, and a 30-day cure period for violations.

Kentucky Consumer Data Protection Act (KCDPA)

Kentucky's law contains coverage thresholds identical to those in the ICDPA: entities in scope control or process personal data on 100,000 consumers or derive 50 percent of revenue from selling the data of more than 25,000 consumers. Businesses subject to the KCDPA must also comply with similar requirements, including data protection impact assessments, consumer opt-out mechanisms, opt-in consent for processing sensitive data, processing standards for deidentified data, and a 30-day cure provision.

Rhode Island Data Transparency and Privacy Protection Act (RIDPA)

Rhode Island's law sets a lower threshold that may bring smaller businesses into scope. The law applies to for-profit entities conducting business in Rhode Island or targeting Rhode Island consumers that either:

- Process personal information of 35,000 or more Rhode Island residents, or
- Process personal information of 10,000 or more Rhode Island residents while deriving more than 20 percent of gross revenue from the sale of personal information.

While Rhode Island's law shares some features with other state privacy statutes, including data subject rights and data protection assessment requirements, it notably excludes several provisions found in other laws. The statute does not include recognition of universal opt-out mechanisms, enhanced children's privacy protections, a definition for personally identifiable information, or a right to cure.

Additionally, the RIDPA imposes a standalone privacy notice requirement on commercial websites and internet service providers that conduct business in Rhode Island or serve Rhode Island customers, regardless of whether they meet the statutory thresholds. These entities must post a notice identifying the categories of personal data collected, disclosing any data sales or targeted advertising, listing third parties to whom data is or may be sold, and providing a contact email address for the controller.

Significant State Law Amendments Effective in 2026

While the three states above are joining the comprehensive privacy compliance landscape for the first time, existing state laws in other states are undergoing equally significant changes that warrant close attention. From dramatically lowered applicability thresholds to eliminated cure periods and new categorical prohibitions, amendments in California, Colorado, Connecticut, Oregon, and Utah signal a clear trend: state privacy enforcement is tightening, and the margin for non-compliance is shrinking. For businesses that thought they were outside the scope of state privacy laws or that had grown comfortable with existing requirements, 2026 brings a critical moment to reassess compliance status and implementation timelines.

California

California continues to enhance its privacy framework with new requirements. Much-discussed California Consumer Privacy Act (CCPA) regulations for automated decision-making technology, risk assessments and cybersecurity audits became applicable at the start of the new year. Additionally, the California Delete Act's delete request and opt-out platform (DROP) launched, raising new data broker requirements and penalties beyond those associated with annual broker registration by the January 31 deadline.

For companies already navigating CCPA compliance, these new regulations demand attention as they refine and expand existing requirements. The automated decision-making technology (ADMT) rules zero in on systems that effectively replace human judgment in consequential decisions affecting consumers. When businesses deploy these tools, they must offer opt-out rights and ensure that any human reviewer can actually understand the system's outputs and has real authority to change the outcome.

Separately, privacy risk assessments are now mandatory whenever processing activities raise potential privacy concerns, such as selling or sharing personal information, handling sensitive data, deploying ADMT for significant decisions, training automated systems for certain uses, or inferring personal characteristics in employment, education, or contractor relationships.

The cybersecurity front also sees important clarifications. New audit rules spell out what qualifies as a "significant risk" triggering audit requirements and establish baseline expectations for reasonable security measures. Breach notification timelines have tightened as well: businesses must notify affected California residents within 30 days of discovering a breach, and if more than 500 people are impacted, the Attorney General must be informed within 15 days of sending consumer notices.

Finally, data brokers subject to the Delete Act must comply with deletion and opt-out requests submitted through the new DROP platform, which applies requests across all registered brokers and requires recurring deletion sweeps. The per-violation penalty structure creates meaningful financial exposure, far exceeding the relatively modest fines for registration failures alone, reflecting California's intensified focus on broker accountability.

Colorado

The Colorado Privacy Act's 60-day right to cure provision reached its sunset on December 31, 2025 – enforcement actions and penalties can proceed immediately without a grace period. Colorado also joined the roster of states requiring recognition of universal opt-out mechanisms as of January 2026. In addition, Colorado's landmark Artificial Intelligence Act regulating high-stakes algorithmic decisions in employment, housing, health care, and financial services has been delayed from February 1 to June 30, 2026.

Connecticut

Effective mid-2026, Connecticut dramatically lowers its applicability threshold from 100,000 to 35,000 customers, significantly expanding the number of businesses subject to the law. The amendments also introduce new categorical requirements including requiring companies processing any sensitive data (such as precise location or financial account information) to comply with the act, regardless of size or customer count. Additionally, companies are prohibited from selling personal data of minors or engaging in targeted advertising to children, regardless of consent. Beginning in January 2026, Connecticut also joins the growing list of states requiring recognition of universal opt-out mechanisms.

Oregon

Building on the Oregon Consumer Privacy Act that became largely effective in July 2024, new provisions took effect January 1, 2026. Controllers are now prohibited from selling geolocation data accurate within 1,750 feet, marking a significant restriction on "precise geolocation data" sales. The amendments also enhance protections for minors by prohibiting controllers from selling personal data of consumers under 16 years old or using such data for targeted advertising or certain types of profiling. Additionally, controllers must now honor consumer opt-out requests made through universal opt-out mechanisms.

Utah

Effective July 1, 2026, Utah consumers will gain a new right to correct inaccuracies in their personal data, with consideration given to the nature of the data and its processing purposes.

Key Takeaways

The state privacy landscape continues to evolve rapidly, with amendments narrowing exemptions, banning new practices, and bringing companies with smaller customer bases into compliance obligations. As

enforcement actions accelerate and cure periods disappear, the stakes for non-compliance have never been higher.

Businesses should treat 2026 as a critical checkpoint.

- Assess whether lowered thresholds now capture your operations.
- Conduct gap analyses to identify where your current programs may fall short of new requirements.
- Prioritize updates to high-risk areas such as sensitive data processing, children's privacy protections, and universal opt-out mechanisms.

Organizations that wait for enforcement letters to prompt action will face not only penalties but also the operational disruption of implementing compliance programs while under regulatory scrutiny.

Navigating this expanding web of state privacy requirements doesn't have to be overwhelming. Whether you're determining if lowered thresholds now apply to your business, conducting data protection impact assessments, assessing procedures for honoring individual privacy rights, implementing universal opt-out mechanisms, or overhauling your entire privacy program to meet new standards, Baker Donelson's Privacy and Data Security Team has the experience to guide you through every step. Contact the authors, Matt White, AIGP, CIPP/US, CIPP/E, CIPT, CIPM, PCIP, Alex Koskey, CIPP/US, CIPP/E, PCIP, and MJ McMahan, or any member of our team, to discuss how we can help you implement practical, cost-effective compliance solutions to navigate these requirements with confidence.