

The Privacy Patchwork Grows: Alabama, Louisiana, Oklahoma, and Vermont Join the Compliance Landscape

OCTOBER 12, 2026

Authors: [Ryan T. Sulkin](#), [Jacob “Jake” Bennett](#)

Featured Practices: [Data Privacy & Cybersecurity](#), [Artificial Intelligence \(AI\)](#), [State Attorneys General Investigations & Enforcement](#), [Technology Transactions](#)

Key Takeaways

- Alabama, Louisiana, Oklahoma, and Vermont have enacted comprehensive consumer privacy laws, further expanding the growing patchwork of state privacy laws in the absence of a federal privacy statute.
- Businesses operating across multiple jurisdictions should not assume that compliance with one state’s comprehensive privacy law automatically satisfies another state’s requirements.
- Businesses should begin reviewing privacy notices, consumer rights procedures, vendor agreements, data governance practices, and sensitive data processing activities in advance of each law’s effective date.

New Privacy Laws at a Glance

State	Effective Date	Applies To	Notable Features
Louisiana	January 1, 2027	Persons or entities doing business in Louisiana that (i) have annual gross revenue > \$25 million; (ii) process the personal data of ≥75,000 Louisiana consumers, households, or devices; or (iii) derive ≥50% gross annual revenue from personal data sales.	Statutory notice requirements for selling sensitive personal or biometric data; opt-in consent for sensitive data processing; 30-day cure period (sunsets July 31, 2027)

Oklahoma	January 1, 2027	Controllers or processors conducting business in Oklahoma that control or process the personal data of (i) $\geq 100,000$ Oklahoma consumers; <u>or</u> (ii) $\geq 25,000$ Oklahoma consumers and derive $>50\%$ of gross revenue from data sales.	Narrower definition of “sale”; 30-day cure period with no scheduled sunset; no opt-out preference signal requirement
Alabama	May 1, 2027	Controllers or processors conducting business in Alabama that (i) control or process the personal data of $>25,000$ Alabama consumers; <u>or</u> (ii) derive $>25\%$ of gross revenue from data sales.	Lower applicability threshold; no data protection assessment requirement; no opt-out preference signal requirement; narrower definition of “sale”
Vermont	January 1, 2028	Persons conducting business in Vermont that (i) control or process the personal data of $\geq 35,000$ Vermont consumers; (ii) control or process the sensitive data of $\geq 3,000$ Vermont consumers; <u>or</u> (iii) sell the personal data of $\geq 3,000$ Vermont consumers.	Separate applicability threshold for consumer health data provisions; LLM disclosure requirements; opt-in consent for sensitive data processing and sales

Common Compliance Framework Across the Four Laws

Although each of these laws contains state-specific requirements, they generally follow the same regulatory framework established by earlier comprehensive state privacy laws, including those in California, Colorado, and Virginia. Accordingly, organizations with existing privacy compliance programs will likely be able to leverage their current policies and procedures rather than develop entirely new compliance frameworks. Each law generally grants consumers the right to access, correct, delete, and obtain copies of at least the personal data they provided to the controller, as well as the right to opt-out of targeted advertising, the sale of personal data, and certain profiling activities.

The discussion below highlights the most significant distinctions among the four new laws.

The Louisiana Data Privacy Act (“LDPA”)

The LDPA becomes effective on January 1, 2027, and applies to persons or entities that conduct business in Louisiana and satisfy at least one of the following thresholds: (1) annual gross revenue exceeding \$25 million; (2) annually buying, receiving, selling, or sharing the personal data of 75,000 or more Louisiana consumers, households, or devices for commercial purposes; or (3) deriving 50% or more of annual gross revenue from selling Louisiana consumers’ personal data. Notably, the LDPA does not apply to entities that merely “target” Louisiana residents with their products and services like many other state laws, which may narrow the law’s reach.

The LDPA’s definition of “sale,” which includes exchanges for monetary or other valuable consideration, is generally consistent with the approach taken by several other state privacy laws. Louisiana follows the emerging trend of requiring opt-in consent for sensitive data processing. The law includes a 30-day cure period before enforcement actions may be initiated, though this cure period sunsets on July 31, 2027. Where the LDPA distinguishes itself is in its requirement for statutory notices when controllers sell sensitive personal data or biometric data. The law also requires data protection assessments for specified high-risk processing activities and mandates recognition of qualifying authorized-agent opt-out requests, including certain browser-based or global privacy preference signals, subject to applicable verification requirements.

The Oklahoma Consumer Data Privacy Act (“OCDPA”)

The OCDPA takes effect on January 1, 2027, and applies to controllers and processors conducting business in Oklahoma that either (1) process the personal data of at least 100,000 Oklahoma consumers annually, or (2) process the personal data of at least 25,000 consumers while deriving more than 50% of gross revenue from the sale of personal data.

Oklahoma distinguishes itself from other recently enacted privacy laws in several principal respects. The OCDPA employs a narrower definition of “sale,” limiting covered transactions to exchanges involving monetary consideration rather than the broader “valuable consideration” standard used by several other states. The law also includes a 30-day cure period before enforcement actions may be initiated, providing businesses with an ongoing opportunity to remediate alleged violations. Notably, this cure period is not currently scheduled to sunset at any point. Additionally, unlike many recently enacted comprehensive privacy laws, Oklahoma does not require companies to recognize opt-out preference signals.

The Alabama Personal Data Protection Act (“APDPA”)

The APDPA takes effect on May 1, 2027, and applies to controllers and processors conducting business in Alabama or producing products or services targeted to Alabama residents that either (1) process the personal data of more than 25,000 Alabama consumers, or (2) derive more than 25% of gross revenue from the sale of personal data. Notably, the APDPA exempts entities with fewer than 500 employees from its scope, provided such entity does not engage in the sale of personal data.

Unlike many state privacy statutes, the APDPA does not require controllers to conduct data protection assessments for heightened-risk processing activities, provide consumers with an appeal

right following the denial of a consumer request, or require recognition of opt-out preference signals. The law does include a 45-day cure period before enforcement actions may be initiated, and notably, this cure period does not sunset. The APDPA does, however, adopt a notably narrow definition of “sale,” capturing only transfers where the controller receives a material benefit and the third party faces no restrictions on subsequent use of the data, and expressly excludes disclosures for analytics services and marketing services solely to the controller.

The Vermont Data Privacy and Online Surveillance Act (“VDPOSA”)

The VDPOSA becomes effective on January 1, 2028, and generally applies to persons that conduct business in Vermont or produce products or services targeted to Vermont residents and meet one of the following thresholds: (1) process the personal data of at least 35,000 Vermont consumers, (2) process the sensitive personal data of at least 3,000 Vermont consumers, or (3) sell the personal data of at least 3,000 Vermont consumers. Its consumer health data provisions are subject to a lower applicability threshold for persons that conduct business in Vermont or target Vermont residents.

Vermont departs most significantly from the traditional state privacy law framework by adopting several requirements that extend beyond those found in many other comprehensive privacy statutes. The law expands consumer rights relating to profiling decisions, restricts certain health data practices, limits geofencing around healthcare facilities for specified purposes, and requires privacy notice disclosure of whether the controller collects, uses, or sells personal data for the purpose of training large language models. Notably, the VDPOSA links its minor protections to Vermont’s separate Age-Appropriate Design Code Act, which takes effect on January 1, 2027, providing that the provisions affording the greatest protection apply when a controller qualifies as a “covered business” under that statute and the consumer is a “covered minor.” The VDPOSA requires opt-in consent before processing or selling sensitive data, including with respect to a known child’s personal data.

Practical Compliance Considerations and Looking Ahead

Because the shared framework still varies in important state-specific ways, businesses should not assume that a single compliance program will satisfy all applicable requirements. As additional states continue enacting comprehensive privacy legislation, businesses should focus on building scalable privacy governance programs that can be adapted to evolving state-specific requirements. Material differences remain with respect to applicability thresholds, opt-out preference signal, appeal rights, data protection assessment obligations, sensitive-data requirements, large language model training disclosures, and enforcement provisions.

The enactment of these four laws brings the total number of comprehensive state privacy laws to 24, further demonstrating that state privacy legislation continues to expand in the absence of a federal privacy statute. While shared principles persist across these statutes, differences continue to multiply, making individualized compliance analyses essential. Organizations that begin evaluating their privacy governance programs now will be better positioned to comply with these laws as they become effective and as additional states continue expanding the U.S. privacy landscape.

* * *

The Benesch Data Privacy & Cybersecurity team continues to monitor developments in state privacy law and advises clients on privacy governance, compliance program development, privacy notices, data processing agreements, AI governance, and regulatory requirements. If you have questions about these laws or their impact on your organization, please contact a member of the team.

** With contribution from David Aronov.*

Ryan Sulkin is Team Lead of Benesch's Data Privacy & Cybersecurity Practice Group. He can be reached at 312.624.6398 or rsulkin@beneschlaw.com.

Jake Bennett is an Associate in Benesch's Data Privacy & Cybersecurity Practice Group. He can be reached at 312.517.9561 or jbennett@beneschlaw.com.