Shumaker

JANUARY 21, 2026 | PUBLICATION

"New Year, New You*! (* - Privacy Laws)

What Businesses Need to Know

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Brian C. Focht

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Contrary to the expectations of many in the privacy field, no new state-level data privacy laws were passed in 2025. As we enter 2026, however, several laws that were passed in 2024, along with several other updates and changes to existing privacy laws and laws governing artificial intelligence (AI) and data breach notification, are taking effect. Here are the new and/or improved laws that businesses need to be aware of in the new year:

I. New Comprehensive State Consumer Privacy Laws Effective January 1, 2026

1) Indiana: Indiana Consumer Data Protection Act (ICDPA)

Effective date: January 1, 2026. (Government of Indiana)

Applies to: Businesses that (1) conduct business in Indiana (or target Indiana residents) and, (2) during a calendar year, either (i) control or process the personal data of 100,000 Indiana consumers, or (ii) control or process the personal data of at least 25,000 Indiana consumers *and* derive more than 50 percent of gross revenue from sale of personal data. The ICDPA contains broad exemptions, including nonprofits and most sectors covered by federal or sector-specific regimes (e.g., Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Billey Act (GLBA)).

Business Obligations: Personal data may only be collected if it is adequate, relevant, and reasonably necessary for the purposes being collected, and consent must be obtained if the personal data is processed for unrelated purposes. Controllers may use data processors pursuant to a written agreement for processing data.

Consumer Rights: Similar to other "comprehensive" state privacy statutes, consumers have the right to access their data, correct incomplete or inaccurate data that was initially provided by the consumer, obtain a copy of the personal data that has been collected, and request that data provided by or obtained about the consumer be deleted. Consumers may make these Data Subject Access Requests (DSARs) on behalf of themselves, their family, or their household.

Consumers may opt out of the processing of personal data for targeted advertising, the sale of their personal data, and the use of personal data for profiling in furtherance of decisions that produce legally significant (or similar) effects.

Businesses must respond to consumer requests within 45 days (with one 45-day extension available) and must provide responses free of charge once per year. Denied requests must be explained and must include a mechanism for the consumer to appeal, and any denial of an appeal must provide information on filing a complaint with the Attorney General.

Enforcement model: Indiana Attorney General is the sole mechanism of enforcement, with a 30-day opportunity to cure following notice. Failure to cure can result in a fine of $7,500 per violation.

What this means in practice: If your organization already built a "Virginia/Colorado/Connecticut-style" privacy program, Indiana is largely an extension. Focus on intake and identity verification, opt-out mechanics, contracting with processors, and appeals.

2) Kentucky: Kentucky Consumer Data Protection Act (KCDPA)

Effective date: January 1, 2026. (Legislative Research Commission)

Applies to: Businesses that (1) conduct business in Kentucky (or target Kentucky residents) and, (2) during a calendar year, either (i) control or process the personal data of 100,000 Kentucky consumers, or (ii) control or process the personal data of at least 25,000 Kentucky consumers *and* derive more than 50 percent of gross revenue from sale of personal data. The KCDPA contains broad exemptions, including nonprofits and most sectors covered by federal or sector-specific regimes (e.g., HIPAA, GLBA).

Business Obligations: Personal data may only be collected if it is adequate, relevant, and reasonably necessary for the purposes being collected, and consent must be obtained if the personal data is processed for unrelated purposes. Controllers may use data processors pursuant to a written agreement for processing data.

Consumer Rights: Similar to other "comprehensive" state privacy statutes, consumers have the right to access their data, correct incomplete or inaccurate data, obtain a copy of the personal data that has been collected, and request that data provided by or obtained about the consumer be deleted.

Consumers may opt out of the processing of personal data for targeted advertising, the sale of their personal data, and the use of personal data for profiling in furtherance of decisions that produce legally significant (or similar) effects.

Businesses must respond to consumer requests within 45 days (with one 45-day extension available) and must provide responses free of charge up to twice per year. Denied requests must be explained and must include a mechanism for the consumer to appeal.

Enforcement model: Kentucky Attorney General is the sole mechanism of enforcement, with a 30-day opportunity to cure following notice. Failure to cure can result in a fine of $7,500 per violation.

What this means in practice: If you are already compliant with Virginia's framework, Kentucky will feel familiar. Confirm your threshold analysis; update your state addendum language; and ensure your DSAR, Data Privacy Impact Assessments (DPIAs), and opt-out workflows extend to Kentucky residents.

3) Rhode Island: Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)

Effective date: January 1, 2026 (webserver.rilegislature.gov).

Applies to: Businesses that (1) conduct business in Rhode Island (or target Rhode Island residents) and, (2) during a calendar year, either (i) control or process the personal data of 35,000 Rhode Island consumers, or (ii) control or process the personal data of at least 10,000 Rhode Island consumers *and* derive more than 20 percent of gross revenue from sale of personal data. The RIDTPPA contains broad exemptions, including nonprofits and most sectors covered by federal or sector-specific regimes (e.g., HIPAA, GLBA).

Business Obligations: Businesses that sell personal data must provide specific information in their privacy notice, including all entities to whom personal data may be sold and a separate notice that personal data may be sold. Controllers may use data processors pursuant to a written agreement for processing data.

Consumer Rights: Similar to other "comprehensive" state privacy statutes, consumers have the right to access their data, correct incomplete or inaccurate data, obtain a copy of the personal data that has been collected, and request that data provided by or obtained about the consumer be deleted.

Consumers may opt out of the processing of personal data for targeted advertising, the sale of their personal data, and the use of personal data for profiling in furtherance of decisions that produce legally significant (or similar) effects.

Businesses must respond to consumer requests within 45 days (with one 45-day extension available), and must provide responses free of charge up to twice per year. Denied requests must be explained and must include a mechanism for the consumer to appeal.

Enforcement model: Rhode Island Attorney General is the sole mechanism of enforcement, with no inherent cure period. Violations constitute a deceptive trade practice under Rhode Island's consumer protection laws, and includes specific fines for intentional disclosures of personal data under certain circumstances.

What this means in practice: Rhode Island's thresholds and some drafting choices differ from the "Virginia model," so don't assume your existing state addendum is drop-in. Check threshold triggers, sensitive data consent, and public disclosures (especially if your business sells personal data!).

II. Other Important Statutory and Regulatory Updates

A) California has several major rule packages and new operational requirements

1) Updated California Privacy Protection Agency (CPPA) regulations

California's CPPA regulations include notable expansions and added detailed frameworks around:

- Automated Decision-Making Technology (ADMT): Businesses must provide consumers with pre-use notices, the right to opt-out (limited exceptions), and rights to appeal. Businesses must also update privacy notices to include ADMT details.
- Cybersecurity Audits and Risk Assessments: Businesses whose processing of personal data presents a significant risk to consumer security must conduct annual cybersecurity audits and produce audit reports. Additionally, qualifying businesses must perform risk assessments analyzing their processing activities and produce risk assessment reports.

Practical Takeaway: Build an internal high-risk processing inventory and a defensible assessment plus audit readiness posture, at minimum.

2) California “Delete Act” (data broker) regulations

California finalized Data Broker Registration and Accessible Deletion Mechanism regulations effective January 1, 2026, including:

- An annual registration fee and payment mechanics (fee set at $6,000 plus payment processing fee caps);
- A defined registration period (January 1–31 of each year); and
- Requirements for data brokers to create and secure accounts and interact with the Delete Request and Opt-Out Platform (DROP), including retrieval of “consumer deletion lists” and account security duties (CPPA)

The DROP program requires the creation of a centralized system through which California consumers can submit deletion requests that reach all registered data brokers simultaneously.

Practical takeaway: If you might be a “data broker” under California’s definition (including complex affiliate structures), this is the moment to (i) confirm status, (ii) register on time, and (iii) operationalize deletion list handling with security controls, logging, and governance.

3) California “geofencing” restrictions near healthcare facilities

California also enacted restrictions aimed at certain location-based practices near healthcare facilities (including sensitive contexts).

Practical takeaway: Review any marketing/advertising location strategies, software development kit (SDK) configurations, and vendor practices that could implicate geofencing in sensitive contexts.

4) California AI laws take effect

AB 316: Liability for AI-Related Harms, AB 325: Algorithmic Pricing and Antitrust, AB 489: Misleading Statements on Health Care Professional Oversight of Artificial Intelligence, AB 621: Expanded Protections Against Digitized Sexually Explicit Deepfakes, and AB 2013: Mandatory Dataset Disclosure for Generative AI Developers all took effect January 1, 2026.

Practical Takeaway: If your business uses AI in any manner that impacts the California market, you should be aware of these new laws. This article will not go into great detail on the implications of each law, but you should be prepared to assess all of your AI tools, particularly those that provide or use algorithmic pricing, ensure risk and liability allocation is prioritized in contract negotiations, and avoid suggesting that AI services are provided by a licensed health care provider when they’re not.

B) Virginia implements social media limits for minors

Virginia enacted a law limiting social media use by minors (commonly described as a “one-hour daily limit”), effective January 1, 2026, and the measure is framed as an amendment interacting with Virginia’s privacy framework (VCDPA).

Practical takeaway: If you operate social media features, youth-oriented services, or ad-tech/engagement tooling with teen users, treat this as both a product/design and privacy compliance issue: age estimation/verification approaches, parental controls, and data minimization will be under a brighter spotlight.

C) Nebraska's Age-Appropriate Online Design Code Act comes into effect

Nebraska's Age-Appropriate Online Design Code law becomes effective January 1, 2026, creating privacy-by-design expectations tied to minor users and likely affecting default settings, profiling, and UX patterns. As with other similar laws, expect this to be challenged in court.

Practical takeaway: If your service is "likely to be accessed by children," audit defaults and dark-pattern risk, and ensure product/engineering has an implementable compliance spec ready to go.

D) Oklahoma breach notification law updates

Oklahoma updated its security breach notification statute via legislation taking effect January 1, 2026.

Practical takeaway: Refresh your incident response plans to reflect updated state notice triggers and timing requirements, and to align vendor notice obligations and cyber insurance reporting workflows.

E) New York: a new sheriff in town (for AI, at least)

New York's Artificial Intelligence Companion Models Law took effect at the end of 2025, and mandates notification and safety protocols for operators of AI "companion" chatbots.

Practical takeaway: If your business uses chatbots in any way, make sure the user knows upfront that they are not talking to a real human. Ideally, find ways to remind them throughout the process and take steps to identify and mitigate potential for causing self-harm.

III. A Practical "Q1 2026" Compliance Checklist

1. Confirm applicability thresholds for Indiana, Kentucky, and Rhode Island (and document your analysis).
2. Extend DSAR workflows (access/delete/correct/copy), including appeals where required.
3. Implement opt-out mechanisms for targeted advertising / sale / profiling.
4. Refresh privacy notices and state addenda (especially Rhode Island's transparency and sale notices and sensitive data consent requirements).
5. If you may be a California data broker, operationalize registration and DROP with security controls and deletion list processing.
6. Assess youth/minor-facing features (Nebraska and Virginia) and ensure your product roadmap includes implementable compliance changes.
7. Update incident response playbooks for Oklahoma (and align contractual breach-notice obligations).
8. Where age verification is implicated (e.g., Missouri contexts), treat it as a privacy engineering project: minimize data, secure it, and shorten retention.

Allow the new year to serve as a reminder that "privacy compliance" is not optional and is no longer about a two-paragraph notice tucked away on your website. Compliance burden aside, however, consumers want to know that you'll protect the data they entrust to you. Let us help you turn privacy into one of your organization's selling points.

Please contact Brian Focht or a member of Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line with questions or for more information.

© 2026 Shumaker, Loop & Kendrick, LLP. All Rights Reserved. Privacy Policy/Disclaimer

Shumaker