1

# Upcoming Privacy Law Review

Look at upcoming major privacy laws and amendments and see if they apply to your organization.

New regulations are evolving past CCPA requirements requiring new privacy rights, artificial intelligence considerations and a greater emphasis on minor, health and biometric data collection.

Reviewed

## Amendment to Montana Consumer Data Privacy Act

**Effective May 8, 2025**

- Reduces minimum thresholds for applicability, particularly for minors
- New privacy notice and disclosure obligations
- Updated requirements for targeted advertising opt-out rights
- Removes 60-day cure period for non-compliance

Notes:

Reviewed

## Reproductive and Sexual Health update to Virginia Consumer Protection Act

**Effective May 8, 2025**

- Much broader applicability than the Virginia Consumer Data Protection Act
- New notice and consent requirements for reproductive or sexual health data collection
- Prohibits businesses from obtaining, disclosing, selling, or disseminating personally identifiable reproductive or sexual health information without consent
- Private right of action for non-compliance

Notes:

Reviewed

## Biometric update to the Colorado Consumer Privacy Act

**Effective July 1, 2025**

- Much broader applicability than the underlying Colorado CPA
- New notice and consent requirements for biometric data collection
- Prohibitions on certain biometric collection from employees

Notes:

Reviewed

## New Tennessee Information Privacy Act

**Effective July 1, 2025**

- Comprehensive privacy law
- Minimum threshold for applicability
- Privacy notice and consent requirements
- Consumer rights with regards to their data
- Requires data processing contracts with vendors
- Requires data protection assessments for high-risk processing

Notes:

Reviewed

## New Idaho Consumer Privacy in Mortgage Applications

**Effective July 1, 2025**

- Requires clear disclosures from companies that purchase trigger leads on how they obtained the consumer information
- Restrictions on the marketing and consumer solicitation techniques companies can use
- Limitations on which companies can use mortgage trigger leads
- Broader definition of “mortgage trigger lead” as compared to the federal Fair Credit Reporting Act (FCRA)

Notes:

Reviewed

## Export of Sensitive and Government Personal Data Final Rule

**Enforcement grace period expires July 8, 2025**

**Due diligence, audit and reporting requirements effective October 5, 2025**

- Prohibits certain transactions involving sensitive personal and government-related data with certain foreign entities and countries, including China
- Restricts other transfers of sensitive personal and government-related data with these certain foreign entities and countries
- Requires data mapping, risk assessments, record retention and vendor management
- Requires implementing the Cybersecurity and Infrastructure Agency Security Requirements

Notes:

Reviewed

## New Minnesota Consumer Data Privacy Act

**Effective July 31, 2025**

- Comprehensive privacy law
- Minimum threshold for applicability
- Privacy notice and consent requirements
- Consumer rights with regards to their data, including rights to:
  - obtain a list of third parties to which the controller has disclosed the consumer's personal data
  - question the results of profiling
  - opt out of targeted advertising/selling data by using universal opt-out mechanisms
- Requires data processing contracts with vendors
- Data protection assessments for high risk processing

Notes:

Reviewed

## Amendment to the Texas Data Broker Act

**Effective September 1, 2025**

- Expands the definition of covered "data brokers" to apply to more businesses
- Requires data brokers operating websites or mobile applications to post clear and accessible notices informing consumers that they are engaging in data brokerage
- Expands the registration requirements for data brokers

Notes:

Reviewed

## New Maryland Online Data Privacy Act

**Effective October 1, 2025**

- Comprehensive privacy law
- Very low minimum threshold for applicability
- Privacy notice and consent requirements
- Consumer rights with regards to their data including the right to opt out of targeted advertising/ selling data by using universal opt-out mechanisms
- Requires data processing contracts with vendors
- Prohibition on the sale of sensitive data
- Requires data protection assessments for high risk processing

Notes:

Reviewed

## Neural and Brain Wave updates to Montana's Genetic Information Privacy Act

**Effective October 1, 2025**

- Adds data generated by activity in the nervous system to the personal information covered by Montana's Genetic Information Privacy Act
- New notice and consent requirements regarding the collection and use of their neural data

Notes:

Reviewed

## New Indiana Consumer Data Protection Act

**Effective January 1, 2026**

- Comprehensive privacy law
- Minimum threshold for applicability
- Privacy notice and consent requirements
- Consumer rights with regards to their data
- Requires data processing contracts with vendors
- Requires data protection assessments for high-risk processing

Notes:

Reviewed

## New Kentucky Consumer Data Protection Act

**Effective January 1, 2026**

- Comprehensive privacy law
- Minimum threshold for applicability
- Privacy notice and consent requirements
- Consumer rights with regards to their data
- Requires data processing contracts with vendors
- Requires data protection assessments for high-risk processing

Notes:

Reviewed

## New Rhode Island Data Transparency and Privacy Protection Act

**Effective January 1, 2026**

- Comprehensive privacy law
- Minimum threshold for applicability
- Privacy notice and consent requirements
- Consumer rights with regards to their data
- Requires data processing contracts with vendors
- Requires data protection assessments for high-risk processing

Notes:

Reviewed

## New Minor Age Verification and Privacy Laws

**State Specific**

### New York Child Data Protection Act

**Effective June 20, 2025**

- Prohibits companies from collecting, sharing, or selling the personal data of children aged 13 to 17 unless they obtain their informed consent or the processing is strictly necessary for specific activities

### Texas App Store Accountability Act

**Effective January 1, 2026**

- Requires app stores to verify users' ages and secure parental consent prior to allowing minors to download apps to their devices

### Social Media amendment to the Virginia Consumer Data Protection Act

**Effective January 1, 2026**

- Require social media platforms to verify users' ages and impose limits of one hour per day for users under the age of 16

### Social Media amendment to the Colorado Consumer Protection Act

**Effective January 1, 2026**

- Minimum user threshold for applicability
- Requires pop-up warning notifications regarding excess social media usage for users under the age of 18
- Does not require age verification by businesses but rather relies on user self-attestation

Notes:

# 2 Update Your Public Privacy Policy

## The consumer public privacy policy is the new face of the modern business.

An updated privacy policy is not only legally required, it is the first thing that regulators, consumer advocates and plaintiffs will look at to probe for weakness in your organization's privacy program.

Review

### What to know

- State by state (and federal) patchwork of privacy regulations require comprehensive and specific privacy notices from most U.S. business
- Transparency and simplicity are the new best practices to ensure not only compliance with privacy law, but as a first line of defense against privacy class actions
- Privacy regulators and consumer advocates are increasing focusing on consumer right mechanisms, like website cookie banners, consent management platforms (CMPs), privacy rights forms and toll-free numbers, and enforcing very nuanced compliance framework with regards to these mechanisms

Completed

- ☐ Update your data collection, processing and disclosures to ensure that they are aligned (and are sufficiently prophylactic) with your growing organization.
- ☐ Ensure your policy covers all privacy laws applicable to your organization in 2025 and early 2026
- ☐ Ensure your policy provides enough transparency for any consents which it supports, especially for high-risk processing and sensitive data collection
- ☐ Update your descriptions of data rights available to consumers. Make sure to update your mechanisms to reflect best practices from recent enforcement.
- ☐ Update your cookies and website technology disclosures to provide transparency on your online tracking practices.

Notes:

3

# Review Your Website Technologies

## It's 2025. Do you know what your website is doing?

Common advertising and analytics technologies deployed in the wrong way or on the wrong sub-pages can cause serious issues with new privacy regulations and class action lawsuits. Invasion of privacy lawsuits are all the rage as crafty plaintiffs deform old laws to apply to new technologies.

Review

### What to know

Common tracking and software technologies are the foundation of a wide variety of privacy-based nuisance lawsuits against website and application operators, especially for high-risk deployments in the consumer healthcare space:

- Illegal pen registers
- Illegal tap and trace devices
- Invasion of privacy claims
- Intrusion upon seclusion claims
- Washington My Health My Data claims
- California Invasion of Privacy Act claims
- Video Privacy Protection Act claims
- Federal and state wiretapping claims

Completed

- ☐ Chatbots that are AI driven or that transmit conversations to third-parties
- ☐ Mobile devices and browsers that capture precise user location without explicit consent
- ☐ Wiretapping and eavesdropping through pixels, session recorders and tracking tools on webpages with sensitive context or data collection fields
- ☐ High risk marketing and analytics pixels, such as the Metal Pixel or TikTok Pixel

Notes:

# Review Your Website Technologies

| Completed | |
|---|---|
| ☐ | Consent management platforms and tools that are not working properly (or at all) |
| ☐ | Cookies that are mislabeled or misclassified |
| ☐ | Session recorder tools that capture keystroke, clicks or screen navigation |
| ☐ | Software Developer Kits (SDKs) that track user location and other data collection without your knowledge |

Notes:

# 4 Implement Your AI Governance Program

## How to balance innovation and risk management in AI is the most difficult question facing organizations.

There is a path forward. Establishing an AI governance framework will allow speedy movement while establishing the necessary guardrails to keep your organization safe.

**Review**

- AI regulation is rapidly developing, focused on:
  - Obtain obtain a list of third parties to which the controller has disclosed the consumer's personal data
  - Preventing bias
  - Rights relating to automated decision-making and profiling
  - Controlling deepfake/synthetic media
  - Requiring bot transparency
  - Anti-deceptive uses and statements
- Transparency is key:
  - Be transparent and don't deceive consumers about how you use AI tools
  - Be transparent about how consumer data is used to train or validate AI tools
  - Be transparent about how AI decision-making impacts a consumer
  - Be transparent about your use or disclosure of AI-generated content (including chat bot interactions)
- If your AI tools make or support significant decisions impacting consumers, have explicitly documented (and followed) policies, procedures and training for ensuring that they are working as intended, evaluating bias and identifying adverse impact to consumers
- Develop and offer mechanisms for consumers to opt-out of decisions made by, or using, AI tools

Notes:

# 4 Implement Your AI Governance Program

| Completed | |
|---|---|
| ☐ | Develop and implement an AI policy that will form the foundation of your AI governance program |
| ☐ | Create and maintain a catalog of approved AI tools along with approved or prohibited uses of such tools |
| ☐ | Perform risk assessment of currently deployed or planned deployment of AI tools for automated decision-making or profiling of consumers |
| ☐ | Update vendor management programs and agreements to require notification of use of AI tools and processes in services |
| ☐ | Comply with transparency obligations including notice of AI use in consumer-facing interfaces (chat bots, recommendation engines or automated screen tools) |
| ☐ | Comply with transparency obligations including notice of AI use in consumer-facing interfaces (chat bots, recommendation engines or automated screen tools) |
| ☐ | Deploy restrictions involving feeding sensitive categories of personal information (e.g. biometric, health or protected class data) into AI tools |
| ☐ | Evaluate consumer opt-out rights related to profiling, automated decision-making or use of AI that has a significant impact on the consumer |

Notes:

5

# Cyber Insurance

In an era where every company is a data company, appropriate coverage for cyber-related events is no longer optional.

Don't wait until you have a potential claim to figure out if you have enough protection from the unexpected.

## Review

### What to know

- Dykema has in-house 20+ years of data privacy/cybersecurity and insurance industry product, claims and underwriting expertise.
- We have successfully coordinated with the appropriately specialized brokers who place cyber insurance coverage (and other lines of critical coverage as our clients' needs dictate). We have also evaluated existing insurance policy limits, terms, pricing and, in many cases, the carrier with which their coverage is placed.
- In light of the extensive and positive feedback that we have received from clients, we are now standardly offering these services at no cost to all of our valued clients.

Notes:

## Asked

- What coverages do I have?
- Is it enough to protect my organization?
- What is excluded?
- Can I chose my own lawyer in the event of a claim?

Notes:

## Incident Response

Our 24/7 Incident Response team assists clients across the U.S. as well as internationally through the entire incident life cycle with our curated panel of expert consultants (forensic, notification, and public relations) that have pre-negotiated rates for Dykema clients; including consultants with expedient turnaround on bitcoin access. Our team also routinely assists clients with security incident containment, managing regulatory compliance and investigations, remediation, and post-event lessons-learned analyses. Our far-reaching network of international privacy counsel also stands ready to assist with localized issues outside the U.S. when needed. Our readily accessible resources and tools help clients quickly evaluate both their U.S. and international regulatory obligations once systems have been restored and forensic investigation has identified any personal data that may have been exposed.

## Litigation

Our team has exceptional experience in successfully defending consumer class actions as well as individual lawsuits asserting a wide range of privacy rights violations and unfair trade practices. These issues frequently arise when a large data privacy or security incident occurs, or a company's business practices are challenged in the collection and usage of consumer information. The Dykema Data Privacy & Cybersecurity Team includes a deep bench of highly skilled and experienced trial, class action and regulatory attorneys who have extensive backgrounds in incident response, multi-jurisdictional litigation and industry regulatory investigations.

## Compliance

We are trusted advisors to our clients on a wide range of compliance matters including data sensitive agreements, drafting data processing agreements, artificial intelligence deployments and privacy disclosures as well as negotiating key vendor contracts. The Dykema team's various areas of expertise and depth of experience are invaluable to our clients in an era of rapidly expanding regulatory requirements for pre-breach cyber security, post-breach response as well as business practices involving the collection and use of consumer information.

## Risk Management

Our Dykema team provides our clients with a comprehensive suite of risk management services, guidance and tools to help them effectively stand up and maintain their strongest risk management protocols. Our broad range of services routinely includes: data breach coaching; information management and litigation readiness; developing and testing incident response plans and privacy policies; regulatory compliance readiness and analysis; third-party management and vendor agreements; and C-suite, board, executive level and employee training.

For more information visit dykema.com/cybersecurity

## Ready to respond to your needs 24/7.

Ready to Respond 24/7

Dykema's Cyber Response Team
877-646-8127

NetDiligence AUTHORIZED BreachCoach

VPO VIRTUAL PRIVACY OFFICER

Dykema

**www.dykema.com**

California | Illinois | Michigan | Minnesota | Texas | Washington, D.C. | Wisconsin