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

Amendments to Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA)

Effective July 1 & October 1, 2026

- Expanded applicability. The threshold drops from 100,000 consumers to 35,000 consumers, and the law now applies to businesses that process sensitive data or sell personal data regardless of processing volume
- Sensitive data requirements become substantially stricter
- Consumers receive enhanced transparency and profiling rights
- Bans on selling precise geolocation
- Establishing new data broker registry
- New restrictions apply to minors' data and targeted advertising
- Privacy notices and governance requirements are expanded

Notes:

Reviewed

Oklahoma Computer Data Privacy Act (OCDPA)

Effective January 1, 2027

- Follows many concepts found in Virginia-style privacy laws
- Creates access, deletion, correction, and portability rights
- Requires opt-outs for targeted advertising and certain data sales
- Data protection assessment requirements
- Sensitive-data consent requirements
- Requires contracts with processors handling personal data

Notes:

[1] A Virginia-style privacy law is a comprehensive state privacy law modeled on the Virginia Consumer Data Protection Act (VCDPA), using a controller/processor framework and granting consumers rights to access, correct, delete, and obtain copies of their personal data, as well as opt out of targeted advertising, data sales, and certain profiling activities. These laws generally require privacy notices, contracts with processors, consent for processing sensitive data, and data protection assessments for high-risk activities, while limiting enforcement to the state attorney general or regulator rather than private lawsuits.

Reviewed

Louisiana Consumer Data Privacy Act (LCDPA)

Effective Date: January 1, 2027

- Follows many concepts found in Virginia-style privacy laws
- Consumer rights for access, deletion, correction, and portability
- Opt-out rights for targeted advertising and data sales
- Sensitive-data consent requirements
- Data protection assessments for high-risk activities
- Requires contracts with processors handling personal data

Notes:

Reviewed

Vermont Age-Appropriate Design Code Act

Effective January 1, 2027

- Applies to covered online businesses likely to be accessed by minors
- Requires highest-privacy default settings for minors
- Requires a duty of care regarding risks such as emotional harm and compulsive use
- Restricts collection, sharing, and retention of minors' personal data beyond what is necessary
- Requires age-assurance processes and transparency around algorithms and data practices

Notes:

Reviewed

California Consumer Privacy Act (CCPA) ADMT Regulations

Effective January 1, 2027

- Businesses using Automated Decision Making Technologies (ADMT) to make significant decisions must comply with the ADMT requirements
- Must inform consumers prior to collection about the specific purpose of the ADMT, logic used, personal information involved, and opt-out rights
- Consumers can opt out of ADMT use for significant decisions (concerning employment, housing, credit, education, or healthcare)
- Consumers can demand details on how the technology evaluated them and outputs generated
- Evaluates whether human reviewers can meaningfully override automated decisions

Notes:

Reviewed

Colorado's Automated Decision-Making Technology Act

Effective January 1, 2027

- Colorado originally enacted the AI Act, but in 2026 the legislature repealed and replaced that framework with the Automated Decision-Making Technology (ADMT) Act, which focuses on automated decision systems used in consequential decisions
- Applies to automated decision-making technology that materially influences "consequential decisions" involving employment, housing, credit, insurance, healthcare, education, and government benefits
- Developers must provide technical documentation describing intended uses, training-data categories, known limitations, human oversight requirements, and material system changes
- Consumers must be informed when ADMT is being used and receive an explanation when an adverse consequential decision is made
- Individuals can request correction of inaccurate data used by the system and seek meaningful human review and reconsideration of adverse decisions

Notes:

Reviewed

Colorado Chatbot Safety Act

Effective January 1, 2027

- Chatbots must clearly disclose that users are interacting with AI rather than a human. Transparency is a core requirement of the statute
- Operators must estimate user age and implement enhanced protections for minors
- Chatbots must implement suicide and self-harm response protocols
- Operators cannot represent chatbot outputs as equivalent to licensed professional advice
- Operators must submit reports to the Colorado Attorney General regarding implementation of required safeguards and response protocols

Notes:

Reviewed

TCPA Global Revocation Rule (Federal)

Effective January 31, 2027

- Adopted as part of the 2024 Report and Order (the Opt-Out Order), which adopted and codified a number of requirements related to TCPA-covered opt-out requests
- In the texting context, certain words *(i.e.*., "stop," "quit," "end," "revoke," "opt out," "cancel," or "unsubscribe" via reply text message) that when sent as a response to a text constitute a *per se* reasonable means to revoke consent
- Must treat a request to revoke consent made by a called party in response to one type of informational message as applicable to all future robocalls and robotexts from that caller on unrelated matters

Notes:

Reviewed

Alabama Personal Data Protection Act (APDPA)

Effective Date: May 1, 2027

- Relatively low applicability threshold compared to many other state laws
- Provide rights to access, correct, delete, and obtain copies of personal data
- Provide opt-outs for certain personal data sales and targeted advertising activities
- Publish a compliant privacy notice
- Obtain consent for processing sensitive data
- Implement controller-processor contractual requirements

Notes:

Reviewed

Amendment to Kentucky Consumer Data Protection Act (KCDPA)

Effective Date: July 1, 2027

- Creates a device specific consent requirement to collect consumer content viewing history data through Smart TV or smart monitor-operated or -embedded ACR technology
- Covers data about a consumer's content viewing history collected through technology embedded in or operated through a smart television or smart monitor that identifies displayed content in real time by analyzing audio or video fingerprints

Notes:

Reviewed

New Jersey Kids Code Act

Effective Date: September 1, 2027

- The law generally applies to larger online service providers that meet revenue or consumer-data processing thresholds and whose services are reasonably likely to be accessed by children or teens.
- Covered services must configure strong privacy protections by default, limit unnecessary collection and sharing of minors' personal information, and implement data minimization practices.
- Limits targeted advertising to minors and places restrictions on the use of children's personal information for recommendation engines, ranking systems, and behavioral profiling.
- Imposes product-design obligations aimed at reducing harm.
- Allows minors (or those acting on their behalf) to bring legal claims for violations

Notes:

Reviewed

Vermont Data Privacy and Online Surveillance Act

Effective Date: January 1, 2028

- Unique application structure that may capture businesses that would be outside the scope of many other state laws
- Consumer access, deletion, correction, and portability rights
- Restrictions on sales and targeted advertising
- Data protection assessment requirements
- Publish a compliant privacy notice
- Obtain consent for processing sensitive data
- Implement controller-processor contractual requirements

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 mid-sized and larger 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

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 2026 and early 2027
- [ ] 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 2026. 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 Meta 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 Prepare for Mandatory Risk Assessments and Cybersecurity Audits

Many businesses are overlooking a critical reality of newest regulations arising out of the California Consumer Privacy Act (CCPA): mandatory assessments, audits and affirmative attestations to the primary California regulator.

Review

What to know

- California's new CCPA regulations create two major new compliance obligations: privacy risk assessments and cybersecurity audits requiring affirmative attestations to the California regulator
- Although the first attestations are not due until April 1, 2028, businesses may need to evaluate processing activities occurring in 2026 and beyond, meaning preparation should begin now
- These requirements are not limited to California-based companies. The CCPA applies to many organizations throughout the United States that do business in California or collect personal information from California residents through websites, mobile applications, ecommerce platforms, customer portals, or digital marketing activities. As a result, businesses headquartered outside California may nevertheless be subject to these new obligations.
- Privacy risk assessments may be required for businesses that engage in certain "high-risk" processing activities
- Certain larger businesses whose processing activities present a significant risk to consumer security may also be required to conduct annual independent cybersecurity audits and submit executive certifications of compliance
- Compliance will require more than a legal review. Businesses should begin:
- Conducting data inventories and mapping exercises
- Identifying covered processing activities
- Reviewing vendor relationships
- Establishing governance and documentation procedures
- Assigning executive ownership and responsibility
- Budgeting for future compliance costs

Notes:

4 Mandatory Risk Assessments and Cybersecurity Audits

Completed

- [ ] Determine whether your organization is subject to the CCPA
  - Assess whether your organization conducts business in California and meets the CCPA's applicability thresholds
  - Consider whether personal information is collected from California residents through websites, ecommerce platforms, customer portals, mobile apps, or marketing activities
- [ ] Conduct a data inventory and data mapping exercise
  - Identify the categories of personal information and sensitive personal information collected, used, disclosed, shared, sold, retained, and processed
  - Map how data flows throughout the organization and to third-party vendors
- [ ] Identify potentially covered processing activities
  - Sale or use of personal information for targeted advertising
  - Use of advertising pixels, cookies, and targeted advertising technologies
  - Processing of sensitive personal information
  - Profiling activities
  - Use of AI or automated decision-making technologies.
  - Use of personal information to train AI or machine-learning system
- [ ] Determine whether privacy risk assessments are requiredSale or use of personal information for targeted advertising
  - Evaluate whether any identified processing activities trigger the new CCPA risk assessment requirements
  - Develop a process to assess new projects before deployment
- [ ] Determine whether cybersecurity audit requirements apply
  - Assess annual revenue thresholds and volumes of personal and sensitive personal information processed
  - Evaluate whether processing activities may present a "significant risk" to consumers' security
  - Determine the organization's applicable audit timeline and compliance deadlines

Notes:

4 Mandatory Risk Assessments and Cybersecurity Audits

Completed

Assign executive ownership

- Designate responsible stakeholders, such as the General Counsel, Chief Privacy Officer, Chief Information Security Officer, Chief Compliance Officer, or other senior executives
- Establish accountability for assessments, audits, record retention, and annual attestations

Establish documentation and recordkeeping procedures

- Develop templates and workflows for risk assessments
- Establish processes for maintaining audit reports, supporting evidence, certifications, and attestations
- Implement retention procedures consistent with regulatory requirements

Budget for compliance

- Estimate costs associated with privacy assessments, cybersecurity audits, consultants, outside counsel, and independent auditors
- Include compliance preparation costs in annual budgeting and planning processes

Conduct a readiness assessment during 2026

- Perform a gap analysis now rather than waiting for 2028 attestation deadlines
- Identify remediation projects, governance improvements, and resource requirements
- Develop a multi-year compliance roadmap

Prepare for future certifications and attestations

- Develop procedures for collecting the information required for annual filings
- Ensure executive leadership receives regular reporting on compliance status
- Establish a process for validating that all required assessments and audits have been completed before certification
- Determine the organization's applicable audit timeline and compliance deadlines

Notes:

5 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:

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)
☐	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:

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 100 YEARS

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