HINSHAW

Don’t Be Spooked by 2026 Privacy Compliance Regulations

View Our Treat of a Roadmap of New California and Colorado Requirements

Privacy, Cyber & AI Decoded Alert | 3 min read

Oct 22, 2025

By: Cathy Mulrow-Peattie, Kelechi Ajoku, Madeline Cook, Sharonda D. Roberson, Claire Standish

As long as you are prepared, there is no need to fear complying with new privacy regulations going into effect in 2026 and beyond. The Halloween 2025 edition of Hinshaw’s *Privacy, Cyber and AI Decoded* covers the newly-approved California Consumer Privacy Act (CCPA) and revised Colorado privacy regulations. Since these regulatory changes will impact most businesses, we cover key takeaways and compliance planning steps for each of these laws below.

California

Consumer Privacy Act Regulations

The California Privacy Protection Agency (CPPA) officially approved the following regulations during its meeting on September 26, 2025. We have provided a summary of these regulations and the expected enforcement dates for internal planning purposes. **These revised regulations impact every business that is subject to the CCPA in some manner.**

Revised CCPA Regulations

What’s New?

- A new definition of sensitive data that includes neural data.
- Clarification that the number of steps for a consumer to opt out of a sale and the sharing of personal information cannot be more than the number of steps to opt in.

What is Required?

- A requirement that a financial incentive program opt-in cannot be more predominant than the ability to opt out.
- Specific guidelines and requirements for the disclosure and sharing of sensitive personal information, including for call centers, brick and mortar stores, through augmented reality, and through connected devices.
- Expanded right-to-know requirements for businesses that collect personal information for more than a 12-month period.
- Expanded requirements for personal information correction, data brokers, and backup system data.
- The requirements should be viewed in light of your organization's current privacy policy disclosures and data subject rights.

Insurance Companies are Now Subject to the CCPA

What's New?

The new CPPA regulations on insurance clarify when insurance companies need to comply with the CCPA.

What is Required?

Effective January 1, 2026, insurance companies meeting the CCPA thresholds must comply with the CCPA for personal information not covered under the California Insurance Code and the Insurance Information and Privacy Protection Act.

- If an insurer processes personal information that is not collected as part of an "insurance transaction" as defined by the California Insurance Code, this information is subject to the requirements of the CCPA.
- This includes marketing information, such as digital tracking cookies or analytics data about consumers who visit the insurer's website, but have not applied for any insurance or financial products, and employee and applicant information.
- Insurance transactional information continues to be governed by the California Insurance Code.

Risk Assessments

What's New?

The CPPA emphasized in its press release that businesses subject to risk assessment requirements must begin

compliance by **January 1, 2026.**

What is Required?

The CPPA regulations require businesses to perform specific regulatory-required privacy risk assessments if their processing of personal information presents a "significant risk" to consumers' privacy.

- Significant risks can include activities such as selling or sharing personal information; processing sensitive personal information; using automated decision-making technologies to make significant decisions, including with relation to employment, biometrics, and financial solutions; and using personal information to train automated decision-making technologies or artificial intelligence.
- The goal of the risk assessment is to restrict or prohibit the processing of personal information if the risks to the privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.
- Businesses engaging in such significant risk activities must now submit the specified information about their risk assessments to the CPPA by **April 2028**, but will cover the time period from January 1, 2026, to December 31, 2027.

Cybersecurity Audits

What's New?

The latest CCPA amendments require businesses presenting a "significant risk" to California consumers to conduct independent, annual cybersecurity audits.

What is Required?

- Businesses are required to document the business's plan to address the gaps and weaknesses identified in the audit regarding potential unauthorized activities, including the timeframe in which it will resolve them.
- These audits must be performed by qualified professionals using recognized standards, with detailed reports and an annual certification submitted to the CPPA, and all audit records must be retained for at least five years.
- The audit mandate will be phased in based on company revenue, with the following deadlines:
  - **April 1, 2028:** For businesses exceeding $100 million in 2026 revenue
  - **April 1, 2029:** For businesses with $50 million to $100 million in 2027 revenue
  - **April 1, 2030**: For businesses with less than $50 million in 2028 revenue

Companies should review their cybersecurity programs for compliance.

Automated Decision-making Technology (ADMT)

What's New?

The CPPA has adopted final regulations on ADMT, creating new compliance obligations for businesses effective **January 1, 2026**. ADMT is defined as any technology that processes personal information and uses computation to fully or substantially replace human decision-making.

What is Required?

The much-debated regulations establish requirements for businesses subject to the CCPA that use ADMT to make significant decisions about consumers, such as the denial of healthcare, financial services, employment, education or housing.

- Compliance is required by **January 1, 2027**, for existing uses, making 2026 compliance planning even more essential.
- Businesses must provide a specific pre-use notice, either as a standalone document or integrated into the notice at collection, explaining the purpose of ADMT, and consumers' opt-out and access rights.

Colorado

Amended Privacy Act Rules

On October 9, 2025, the Colorado Department of Law adopted several new rules, as itemized below, after a significant comment period regarding the online personal data of minors. The Department of Law has asked for a formal opinion on the adoption of the Rules from the Colorado Attorney General. After the formal opinion is issued and the Rules are filed with the Colorado Secretary of State, they will become effective in 30 days.

Duty with Regard to Minors-Knowledge Standard

What's New?

The Rules adopt a clarification on when a controller has knowledge that it is marketing to consumers. This includes the fact that the online ads are directed to minors or that the website's consumers are considered minors, but the new Rules are clear, and age verification technology is not required.

Minor Design Standards

What's New?

The Rule requires that certain factors may be considered when determining if a system design feature significantly increases, sustains, or extends a minor's use of an online service, product, or feature and is subject to the consent requirements of the Rules.

What is Required?

Consent is required from the minor unless the system design features satisfy the broad exceptions, which include:

i. the minor's search inquiries;
ii. if the system design feature is one that is necessary to the core functionality of an online service, product, or feature;
iii. if the system design feature is based on information that is personal data that is not persistently associated with the minor or the minor's device; and
iv. if the online service, product, or feature contains countervailing measures that could mitigate the harm or other negative effects of the system design feature, such as default time of day or time use limits, or required parental controls.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Related People

Kelechi Ajoku

Associate

212-655-3837

Madeline Cook

Associate

212-655-3809

Cathy Mulrow-Peattie

Partner

212-655-3875

Sharonda D. Roberson

Associate

945-229-6369

Claire Standish

Associate

212-655-3842

Related Capabilities

Consumer Financial Services

Data Breach

Data Privacy, AI & Cybersecurity

Financial Services

Healthcare

Insurance

Website Data Privacy

Related Insights

New CPPA Decision Means Businesses Must Review Their Privacy Compliance Processes and Consent Management Tools

AI Moratorium, Bulk Data Controls, and Enforcement Trends

Fall 2025 Regulatory Roundup: Top U.S. Privacy and AI Developments for Businesses to Track