
# Mark Your Calendars! Upcoming Compliance Dates in State Privacy Laws

Aaron J. Burstein, Alexander I. Schneider, Meaghan M. Donahue

September 29, 2025

Although no state has enacted a new comprehensive privacy law in 2025, laws in a few states will soon go into effect, and amendments to existing laws and new regulations abound.

**Just this summer alone, the CPPA finalized new regulations setting requirements for risk assessments, cybersecurity audits, and automated decision-making (ADMT**); Colorado amended its AI Act to delay the law's effective date by five months; and states with privacy laws already in place passed amendments beefing up their compliance obligations. In addition, new laws in Maryland, Indiana, Kentucky, and Rhode Island are set to take effect in the next six months and will introduce a few new compliance wrinkles.

Now more than ever, it's critical to keep an eye on effective dates and prepare for upcoming regulatory requirements. Below, we provide a state-by-state summary and a timeline of some of the key dates and obligations to add to your calendar.

**1. California CCPA Regulations & DELETE Act Regulations:** In July, the California Privacy Protection Agency (CPPA) finalized new CCPA regulations, amending existing requirements and adding new obligations related to risk assessments, cybersecurity audits, and ADMT. Additionally, regulations implementing California's data broker-focused law, the DELETE Act, will go into effect next year.

### Risk assessments:

**What?** – Businesses will be required to conduct risk assessments before engaging in processing activities that present a "significant risk" to consumer privacy, including uses of ADMT for significant decisions concerning a consumer. Risk assessments must include information on the categories of personal information being processed and the purpose for that processing, the methods of processing, the duration of processing, the retention period for the relevant personal information, expected benefits and negative impacts, etc. If relevant processing activities materially change, the corresponding risk assessment must be reviewed and updated within 45 days of the change. Even if their processing activities do not change, businesses must review and update as necessary their existing risk assessments.

**When?** – Businesses will need to begin conducting risk assessments for new processing activities beginning **January 1, 2026.** Per the CPPA's press release, for processing activities that are initiated before January 1, 2026 and continue after this date, businesses must conduct initial risk assessments

no later than December 31, 2027;and submit initial risk assessment reports to the CPPA by April 1, 2028.

**Cybersecurity audits:**

**What?** – Businesses must conduct annual cybersecurity audits when their processing of personal information presents a "significant risk" to security by meeting either of two thresholds:

Threshold 1: The business derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

Threshold 2: The business had annual gross revenues in excess of $26.6 million, as adjusted annually for inflation, and either (a) processed personal information of 250,000 or more consumers or households or (b) processed sensitive personal information of 50,000 or more consumers or households in the preceding calendar year.

Cybersecurity audits must be performed by a "qualified, objective, independent professional" auditor and must assess authentication and encryption practices, account management and access controls, inventory and management of personal information, vulnerability scanning, segmentation of information, cybersecurity education, and other similar factors.

**When?** – The initial audit submission deadline is based on annual gross revenue:

- Annual gross revenue greater than $100 million - **April 1st, 2028**.
- Annual gross revenue between $50-$100 million - **April 1st, 2029**.
- Annual gross revenue less than $50 million - **April 1st, 2030.**

**ADMT:**

**What?** – These regulations apply to businesses using ADMT to make "significant decisions" concerning consumers. A "significant decision" is one that results in the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services, as further defined in the CCPA regulations. "Significant decisions" do not include advertising to a consumer. (However, the California Civil Rights Council adopted recently amended its existing anti-discrimination regulations to expressly cover the use of "automated-decision systems" to "direct[] job advertisements or other recruiting materials to targeted groups.)" Businesses engaging in ADMT must also provide a pre-use notice and allow consumers to opt-out of ADMT processing.

**When?** – Obligations effective beginning **January 1, 2027**.

### Amendments to existing CCPA regulations:

**What?** – The updated regulations tweak existing obligations regarding privacy disclosures, fulfillment of privacy rights requests, and contract terms.

**When?** – New obligations are effective beginning **January 1, 2026**.

### DELETE Act regulations:

**What?** – The DELETE Act requires the CPPA to establish by January 1, 2026 a one-stop mechanism that allows consumers to send a deletion request to every data broker registered in the state.  On

September 26, 2025, the CPPA adopted regulations specifying the details of this mechanism, known as the Delete Request and Opt-Out Platform, or "DROP." Initially published for public comment on April 25, 2025, the DROP regulations, among other things, set requirements for data brokers to register with the platform, specify the formats of deletion lists, and establish fees to access the platform. Data brokers must access the deletion mechanism at least once every 45 days, delete all personal information that they can match with identifiers associated with the consumers making requests, and direct their service providers and contractors to do the same.

**When?** – Obligations effective beginning **August 1, 2026**.

**2. Colorado AI Act:** Originally passed in May 2024, the amendments signed in August 2025 businesses more time to come into compliance.

**What?** – The Colorado AI Act imposes a duty of reasonable care and disclosure obligations on developers and deployers of "high risk" AI technology (i.e., AI-systems making or substantially influencing consequential decisions related to employment, education, finance, housing, healthcare, etc.). Additionally, any business that makes an AI system available for a consumer to interact with must provide the consumer with notice disclosing that fact.

**When?** – Obligations effective beginning **June 30, 2026** (pushed back from February 1, 2026).

### 3. Comprehensive Privacy Laws:

### Maryland:

**What?** – The state's comprehensive privacy law will apply to businesses that control or process the personal information of 35,000 Maryland consumers, or that process the personal information of 10,000 Maryland consumers and derive more than 20% of gross revenue from the sale of personal information. Additionally, the law limits the collection of personal information to that which is "reasonably necessary or proportionate" to provide the specific product or service and bans the sale of sensitive personal information.

**When?** – Effective **October 1, 2025**.

### Montana:

**What?** – Recently signed amendments to the state's privacy law remove the entity-level GLBA exemption and impose a duty of reasonable care to avoid heightened risk of harm if an online service that is offered to a user the business actually knows or willfully disregards is under 18.

**When?** – Amendments effective **October 1, 2025**.

### Indiana:

**What?** – The requirements in Indiana's new law are substantively identical to obligations already provided in other states.

**When?** – Effective **January 1, 2026**.

### Kentucky:

**What?** - The requirements in Kentucky's new law are substantively identical to obligations already provided in other states.

**When?** - Effective **January 1, 2026**.

## Oregon:

**What?** – Recently signed amendments to the state’s privacy law prohibit the sale of personal data linked or linkable to an individual that can be used to identify the individual’s past or present location within 1,750 feet; consent is not an option.

**When?** – Effective **January 1, 2026**.

## Rhode Island:

**What?** – Rhode Island's law will require businesses to post a publicly available list of the third parties with which they disclose personally identifiable information on their websites, in addition to obligations already required by other state privacy laws.

**When?** – Effective **January 1, 2026**.

## Connecticut:

**What?** – Recently signed amendments expand the applicability of the state’s law to any business that controls or processes sensitive personal data or offers a consumer’s personal data “for sale in trade or commerce” (even if the business does not meet other thresholds in the law). The amendments also remove the entity level-GLBA exemption, impose new obligations on companies engaged in profiling or automated decision making, and add the right to request a specific list of the third parties to which the business disclosed the consumer's personal data.

**When?** – Amendments effective **July 1, 2026.**

Click here for a pdf version of the timeline.