Insights, News & Events

NEW CALIFORNIA REGS WILL IMPACT YOUR AI AND PRIVACY POLICIES: FAQS ON AUTOMATED DECISION-MAKING, RISK ASSESSMENTS, AND CYBERSECURITY AUDITS

Insights
Jul 31, 2025

California regulators unanimously approved a sweeping set of regulations on July 24 governing the use of automated decision-making technology (ADMT) and mandating risk assessments and cybersecurity audits for businesses subject to the California Consumer Privacy Act. The regulations will impose significant new obligations on businesses regarding pre-use notices, opt-out rights, annual cybersecurity audits, and detailed risk assessments. The California Privacy Protection Agency (CPPA) must now submit the regulations to the Office of Administrative Law, which has 30 working days to review them for compliance with the Administrative Procedure Act. Approval is expected. We'll explain the new requirements for covered businesses and provide key action items to help you comply.

Automated Decision-Making Technology (ADMT)

What is an ADMT?

An ADMT is any technology that processes personal information and uses computation to replace or substantially replace human decision making. This definition captures a broad range of tools, including resume screeners, performance scoring systems, scheduling software, productivity monitoring applications, and any system used to influence hiring, promotion, compensation, or discipline. Given the "substantially replace" language, businesses cannot rely on nominal human review to avoid compliance.

Related People

Darcey M. Groden, CIPP/US

Partner

858.597.9627

Chelsea Viola

Associate

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

Didn't the California Civil Rights Department already issue regulations on ADMTs?

Earlier this summer, the California Civil Rights Department (CRD) finalized regulations on "automated decision technology," a term that closely mirrors ADMT, in the context of employment decisions. The CRD rules prohibit using such tools to consider protected characteristics and are aimed at preventing discrimination in hiring, promotion, compensation, and other employment practices. You can read more about those regulations here.

These new regulations will not supplant the CRD regulations. Rather, for businesses subject to the California Consumer Privacy Act, these new CCPA regulations are additional. The CRD regulations are limited in scope compared to the CPPA's and apply only in the job applicant and employment contexts.

Is my use of spell check or grammar software regulated by the CPPA?

No. The CPPA is regulating any ADMT used to make a "significant decision."

What is a significant decision?

A significant decision results in the provision or denial of the following services:

- Financial or lending services (the extension of credit or a loan; transmission or exchanging funds; the provision of deposit or checking accounts; check cashing; or installment payment plans).
- Housing, although the use of an ADMT that provides or denies housing to a consumer based solely on the availability or vacancy of the housing or the successful receipt of payment for housing from the consumer is not making a significant decision.
- Education enrollment opportunities (admission or acceptance into academic or vocational programs; educational credentials such as a degree, diploma, or certification; and suspension or expulsion).
- Employment or independent contracting opportunities or compensation (hiring; allocation/assignment of work and

213.403.9626

David J. Walton, AIGP, CIPP/US

Partner

610.230.6105

Service Focus

AI, Data, and Analytics

Consumer Privacy Team

Data Protection and Cybersecurity

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

compensation; promotion; demotion, suspension, and termination).

- Healthcare services.

My business uses ADMTs to make significant decisions; do I have to provide any kind of notice?

Yes. Before deploying ADMT for significant decisions, businesses must issue a clear and accessible pre-use notice to affected individuals, including job applicants and employees. They must explain:

- the purpose for which the ADMT is being used;
- how to opt out (or, if there is an exception to the opt-out right, an explanation of how to appeal the ADMT decision to a human reviewer);
- a description of the consumer's right to access relevant ADMT data and how to exercise that right;
- non-retaliation rights under the California Consumer Privacy Act;
- and a description of how the ADMT works to make a significant decision and how the significant decision would be made if the consumer opts out.

When do I have to comply with the ADMT regulations?

If you are currently using ADMT for significant decisions, you have until January 1, 2027, to issue compliant notices. For any new deployment of ADMT on or after January 1, 2027, the notice must be provided before the technology is used.

What are my next steps for compliance with ADMTs?

✓ **Identify all ADMTs used to make significant decisions.** This is easier said than done, as it will require reviewing processes through the entire business to identify ADMTs. We strongly recommend you start on this now.

✓ **Prepare pre-use notices to consumers when significant decisions are made through ADMTs. These notices are not plug-and-play.** They should be customized to address the particular constituent and the ADMT used. While you can

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

consolidate pre-use notices, businesses would be wise to consider the proper constituents of the notice.

✓ **Update your consumer response processes** and be prepared to address opt-outs from ADMTs, appeals to a human reviewer where opt-outs are not permitted, and requests to access ADMT. And, keep in mind, despite the popularity of cookie banners right now, they are not the proper mechanism for pre-use notification or submitting consumer requests relating to ADMTs.

Risk Assessments

What is a risk assessment?

In some circumstances, businesses will need to analyze whether the risks to consumers' privacy from processing personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public. If the risks outweigh the benefits, the business should not process personal information in that context or for that use.

When does my business need to conduct a risk assessment?

Businesses must conduct a risk assessment before engaging in any activity that presents "a significant risk to consumers' privacy." The regulations highlight the following activities:

- Selling or sharing personal information.
- Processing sensitive personal information, although risk assessments are not required for businesses that process sensitive personal information of employees or independent contractors for the sole purposes of administering compensation payments, determining and storing employment authorization, administering employment benefits, providing reasonable accommodation as required by law, or wage reporting as required by law.
- Using ADMT to make significant decisions about consumers. A good rule of thumb is that if you have to provide a pre-use notice under the ADMT regulations, you will need to conduct a risk assessment regarding that ADMT.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

- Using automated tools to infer or analyze traits like intelligence, mental health, reliability, or performance based on systematic observation of employees, job applicants, students, or independent contractors.
- Using automated processing to draw similar inferences based on a consumer's presence in sensitive locations, such as medical facilities, religious sites, or political events.
- Processing personal information that the business intends to use (or allow others to use) to train ADMT for significant decision making, emotion or facial recognition, identity verification, or biometric profiling.

My business conducted a risk assessment to comply with other states' consumer privacy laws. Do I need to do a separate one for California?

Yes and no. The CPPA permits businesses to do one risk assessment to comply with multiple state consumer privacy laws (or other purposes), providing that the risk assessment contains all the information required by the CPPA's new regulations. The CPPA has many more requirements that other consumer privacy laws. As such, if your business did a risk assessment for another state already, it is likely not compliant with the California requirements. But, moving forward, you can do a single risk assessment, provided it addresses everything required by the CPPA regulations.

When do I have to complete a risk assessment?

For any current practices in place before the regulations take effect, a risk assessment must be completed by no later than December 31, 2027. Otherwise, a risk assessment must be reviewed and updated every three years. If there is a material change to a processing activity, the risk assessment must be updated as soon as feasible, but no later than 45 calendar days from the date of the material change.

What are my next steps for compliance with risks assessments?

✓ **Identify all processing activities that may require a risk assessment.** Review processes through the entire business to identify any significant risk to consumer privacy. If your website has tracking technology that sells or shares

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

personal information, be aware that will give rise to the need to conduct a risk assessment. We strongly recommend you start on this now.

✓ **Reach out to experienced legal counsel.** Risk assessments require a business to make a multitude of considerations and involve certain stakeholders. Given the complexity of risk assessments, this is likely something your business does not want to do alone.

✓ **Submit your risk assessment to the CPPA on time.** For risk assessments completed in 2026 and 2027, they must be submitted no later than April 1, 2028. For risk assessments completed after 2027, they must be submitted by no later than April 1 of the following calendar year.

✓ **Create a system to capture material changes or new processing activities** prompting an update to the risk assessment.

Cybersecurity Audits

What businesses need to complete cybersecurity audits?

Businesses that engage in processing activities that present a "significant risk to consumers' security" must complete a cybersecurity audit. An audit will be required if:

- The business derived 50% or more of its annual revenue in the prior calendar year from selling or sharing personal information; or
- The business is subject to the California Consumer Privacy Act for meeting the revenue threshold (currently $26,625) and:
  - Processed the personal information of 250,000 or more California consumers or households in the prior calendar year; or
  - Processed the sensitive personal information of 50,000 or more California consumers in the prior calendar year.

My business engages in activity that presents a "significant risk to consumers' security." When does my business need to complete its first cybersecurity audit?

Cybersecurity audits will be phased in starting in 2028, and the timing of your first required cybersecurity audit depends

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

on your business's gross annual revenue:

- If your annual gross revenue exceeded $100 million in 2026, your first audit is due by **April 1, 2028** (covering January 1, 2027, through January 1, 2028).
- If your annual gross revenue was between $50 million and $100 million in 2027, your audit is due by **April 1, 2029** (covering January 1, 2028, through January 1, 2029).
- If your revenue was under $50 million in 2028, your audit is due by **April 1, 2030** (covering January 1, 2029, through January 1, 2030).

How frequently does my business need to do a cybersecurity audit?

Annually for as long as your business meets the criteria to require an audit for the prior calendar year.

What are my next steps for compliance with cybersecurity audits?

✓ **Identify if and when your business is likely to be subject to a cybersecurity audit, and be prepared to retain a qualified cybersecurity professional at that time.** If you have an internal auditor who meets the CPPA's qualifications, review whether you have processes in place to ensure the auditor's independence.

✓ **Consider conducting a cybersecurity audit now.** Auditors will need to rely on evidence, rather than assertions from management. As such, conducting a dry run a year or two in advance will allow the business to develop processes to obtain necessary information and complete the audit within the required time frame in the future. Additionally, conducting audits now will allow the business to identify any gaps and fix them sooner rather than later.

Conclusion

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. You can also visit FP's US Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Consumer

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

Privacy Team, Data Protection and Cybersecurity Team, or AI, Data, and Analytics Team.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.