WILLKIE

CLIENT ALERT

CPPA Approves Regulations on Automated Decisionmaking Technologies, Cyber Audits, Risk Assessments, and Insurance Companies

August 11, 2025

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Susan Rohol | Michelle (Eun Jung) Bae

Key Takeaways

- The California Privacy Protection Agency ("CPPA") adopted broad and potentially cumbersome regulations on "automated decisionmaking technologies" ("ADMT"), cybersecurity audits, and risk assessments. The effective date of the new regulations may be as early as October 1, 2025—subject to certain administrative approvals that must be secured. The CPPA has also established specific compliance dates for each of the new requirements.

- The CPPA attempted to distinguish between ADMT and artificial intelligence, but the practical result is that the ADMT rules will usher in significant notice and consumer rights requirements where artificial intelligence is used for "significant decisions," such as eligibility for financial products, as well as decisions on employment, healthcare, or educational opportunities. And the other new rules will require cybersecurity audits for a broad array of large and small companies, including companies with revenues under $50 million,

as well as risk assessments for any data processing activity that carries "significant risk," such as any data processing that involves sale or sharing of personal information (including most personalized advertising).

- More broadly, these regulations address issues that overlap with similar regulations and requirements already in place or being adopted in other states, sometimes in ways that introduce different requirements. For example, the risk assessment rule addresses many of the same issues covered by similar requirements in other state privacy laws, but minor differences in scope, how to factor benefits versus risks, and other aspects of the rule, are likely to increase significantly the costs and complexity of compliance for many companies.

Background

On July 24, 2025, the CPPA Board approved the California Consumer Privacy Act ("CCPA") regulations on ADMT, cybersecurity audits, and risk assessments (the "New Regulations").[1] These New Regulations impose substantial obligations that companies doing business in California will need to carefully review and understand to ensure they are compliant. Below, we provide a summary of each of the major New Regulations, focusing on who is covered, what is required, when the requirements come into effect, and any key differences between what CPPA adopted and similar requirements in other jurisdictions.

The New Regulations

(1) Automated Decisionmaking Technologies

Which businesses are subject to the new ADMT requirements? Any business that uses ADMT to make a "significant decision" concerning a consumer must comply with the New Regulations. ADMT—the statutory term that the CPPA uses instead of "artificial intelligence"—is defined as "any technology that processes personal information and uses computation to replace human decisionmaking, or substantially replace human decisionmaking." And a "significant decision" is defined as a decision 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.

What are the new ADMT requirements? There are two critical requirements:

Pre-use notice. A covered business must provide a "Pre-Use Notice" to consumers. This notice must include, among other things, an explanation of the specific purpose for which the business plans to use

[1] Modified Text of Proposed Regulations (July 2025), the California Privacy Protection Agency, available here. The CPPA concurrently approved regulations focused on insurance companies that, according to the CPPA, are intended to "clarify existing requirements under the CCPA and respond to concerns regarding the personal information collected, used, processed, or retained by insurance companies that are not subject to the Insurance Code and other laws, such as the federal Gramm-Leach-Bliley Act." Draft FSOR Appendix A – Summaries and Responses to 45 Day Comments, the California Privacy Protection Agency, available here at 348 ("Summaries and Responses to 45 Day Comments").

ADMT, a description of the right to opt out of ADMT and how a consumer can exercise that right, and information about how the ADMT works.

Consumer rights. The New Regulations require the business to provide consumers a right to access information about the ADMT, as well as a right to opt out of use of the ADMT. A business is not, however, required to provide such an opt-out under certain circumstances, such as if it provides the consumer with a method to appeal the decision to a human reviewer with authority to overturn the decision. The New Regulations also require providing specific information to the consumer about the logic of the ADMT and the outcome of the decisionmaking process.

When do companies need to be compliant? A business that uses ADMT to make a significant decision prior to January 1, 2027 must be in compliance with the New Regulations by January 1, 2027.

What's different? The CPPA ultimately decided to remove any explicit references to "artificial intelligence," but the parallels between these rules and AI-specific rules enacted in the European Union and Colorado, as well as those under consideration in numerous other states (including California's legislature), are readily apparent. Companies hoping for a reprieve from the patchwork nature of privacy laws in the U.S. will find no relief here, as this rule suggests the potential for multiple sets of AI-focused requirements even within a single state. For example, several commentators noted that the new ADMT rules do not align with existing privacy regimes, such as the ADMT's broad definition of "significant decision" or the broad opt-out right, compared to the similar requirement under the GDPR. In response, the CPPA stated that the proposed definitions of ADMT and significant decision "are clear and not overly broad," and that the New Regulations "are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses."[2] Similarly, in response to a public comment that the CCPA's pre-use requirement is more stringent than comparable privacy laws, the CPPA disagreed and explained that the new requirement "harmonizes with other laws while furthering the purposes of the CCPA and providing clarity to businesses about their obligations."[3]

(2) Cybersecurity Audits

Which businesses are required to conduct a CCPA cybersecurity audit? A business whose processing of consumers' personal information presents "significant risk" to consumers' security must conduct a cybersecurity audit. However, "significant risk" is not defined in terms of the risk to the consumer, but in terms of the amount and type of data being processed—a business is covered by this requirement if, in the preceding calendar year, it processed (i) the personal information of 250,000 or more consumers or households or (ii) the sensitive personal information of 50,000 or more consumers or households.[4]

What must a cybersecurity audit cover? A cybersecurity audit must assess the business's cybersecurity program, including written documentation such as policies and procedures, and the implementation and

2 *Summaries and Responses to 45 Day Comments* at 236.

3 *Id.* at 217.

4 The New Regulations do not specify whether these thresholds should be calculated using just California consumers or households or overall consumers or households.

maintenance of the program. The New Regulations list 18 components of a cybersecurity program that must be assessed, including: authentication (including multi-factor authentication), encryption, access controls, internal and external vulnerability scans and penetration testing, cybersecurity training, service provider oversight, data retention, business continuity and disaster recovery plans, and incident response.[5]

Companies must produce a cybersecurity audit report that includes the specific evidence examined to make decisions and assessments, and the status of any gaps or weaknesses in policies and procedures and the business's plan to address any such gaps. The auditor must be qualified, objective, and independent, using procedures and standards accepted in the profession of auditing. The auditor can be either internal or external, but if a business chooses to use an internal auditor, the highest-ranking auditor must report directly to a member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program.

Finally, each covered business must submit to the CPPA by April 1 of each calendar year a written certification that it has completed the cybersecurity audit. The certification must be completed by a member of the business's executive management team who is directly responsible for the business's cybersecurity compliance and has sufficient knowledge of the audit to provide accurate information.

When do companies need to file their first certifications? The CPPA established a series of compliance deadlines based on a business's annual gross revenue:

- Businesses with annual gross revenue of over $100 million must submit their initial certification by April 1, 2028;
- Businesses with annual gross revenue between $50 million and $100 million must submit their initial certification by April 1, 2029;
- Businesses with annual gross revenue of less than $50 million must submit their initial certification by April 1, 2030.

What's different? These new requirements are generally consistent with the growing trend to require documented data protection and cybersecurity programs, but the details will matter. Small differences between these rules and the SEC's requirements for public company registrants, or the requirements of New York Department of Financial Services Cybersecurity Regulation, will likely be magnified and force companies to consider additional steps as part of their cybersecurity audit and governance. And companies in the financial, healthcare, and similar sectors should not rest easy on compliance with existing laws; the CPPA emphasized in its responses to comments that although the CCPA includes data-level exemptions, including for information subject to the GLBA and HIPAA, the CCPA

[5] These components are largely similar to the areas that must be addressed in policies and procedures for companies that are subject to the NYDFS Cybersecurity Regulation.

nevertheless applies to CCPA "businesses"—those processing personal information subject to the CCPA that falls outside of the "data level" exemption—and "is intended to supplement federal and state law."[6]

(3) Risk Assessments

Which businesses must conduct a risk assessment? A business whose processing of personal information presents "significant risk" to consumers' privacy must conduct a risk assessment before initiating that processing. Among other things, processing presents "significant risk" when it involves any of the following activities: (1) selling or sharing personal information; (2) processing sensitive personal information (other than processing employee data for certain HR purposes); or (3) using ADMT to make a significant decision concerning a consumer.

What must the risk assessment cover? The risk assessment must determine whether the risks to a consumer's privacy from the proposed processing activities outweigh the benefits to the consumer, the business, other stakeholders, and the public from those activities. As part of making such a determination, the New Regulations identify different factors that should be considered, including: the purpose for processing, categories of personal information to be processed, operational elements, the benefits of the processing, the negative impacts to consumers' privacy associated with the processing, and safeguards to be implemented.

To demonstrate compliance, businesses must submit an attestation to the CPPA by April 1 following any year during which the business conducted a risk assessment, attesting that the business has conducted a risk assessment that meets the requirements of the New Regulations. The attestation must be submitted by a member of the business's executive management team who is directly responsible for the business's risk assessment compliance and has sufficient knowledge of the business's risk assessment, and must include the number of risk assessments conducted or updated during the time period covered by the submission.

When must companies have their initial assessments completed? For processing activities covered by these requirements that a business already undertakes and plans to continue past December 31, 2027, the business must have conducted and documented its risk assessment by December 31, 2027. Initial attestations must be submitted by April 1, 2028, for risk assessments conducted in 2026 and 2027. Risk assessment must be reviewed and updated at least once every three years, or, if there is a material change to the processing activity, within 45 days of the material change.

What's different? Companies complying with other state privacy laws, such as those in Virginia and Colorado, will have experience conducting similar assessments, but the scope and many of the details of the New Regulations will force companies to reconsider exactly how they conduct those assessments. The CPPA attempted to address concerns about the additional costs and complexities associated with yet another risk assessment for data processing activities by allowing businesses to utilize risk assessments prepared for another purpose to comply with the New Regulations, but those other risk assessments will suffice only if they contain *all* the risk assessment elements that are required under the New Regulations.

---

6 *Summaries and Responses to 45 Day Comments* at 289.

Next Steps

To finalize the New Regulations, the CPPA must submit the final rulemaking package to the California Office of Administrative Law ("OAL"); the OAL has 30 calendar days to approve and then file the package with the California Secretary of State. Because the effective date of a regulation is generally the first day of the quarter following its submission to the Secretary of State, if the CPPA files the final regulations with the OAL by August 31, 2025, the New Regulations will take effect on October 1, 2025. If the filing is made after August 31 and before November 30, the New Regulations will take effect on January 1, 2026.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez	Laura E. Jehl	Susan Rohol	Michelle (Eun Jung) Bae
202 303 1125	202 303 1056	310 855 3172	212 728 3166
dalvarez@willkie.com	ljehl@willkie.com	srohol@willkie.com	ebae@willkie.com

WILLKIE

BRUSSELS CHICAGO DALLAS FRANKFURT HAMBURG HOUSTON LONDON LOS ANGELES
MILAN MUNICH NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON

Copyright © 2025 Willkie Farr & Gallagher LLP. All rights reserved.

This alert is provided for educational and informational purposes only and is not intended and should not be construed as legal advice, and it does not establish an attorney-client relationship in any form. This alert may be considered advertising under applicable state laws. Our website is: www.willkie.com.