MINTZ

CPPA Regulations Are Moving Forward: Here is What You Need To Know

August 11, 2025 | Blog | By **M. Bertie Magit**, **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

- Privacy & Cybersecurity

RELATED INDUSTRIES

Consumer protections have expanded in California following the approval of the California Consumer Privacy Act ("CCPA") regulations ("Regulations") by the California Privacy Protection Agency ("CPPA"). The Regulations, updating certain existing CCPA regulations and introducing regulations regarding automated decision-making technology ("ADMT"), risk assessments, and cybersecurity audits, will go into effect as early as January 1, 2026, pending review by California's Office of Administrative Law.

The Regulations will require many businesses utilizing ADMT, and/or processing, selling, or sharing personal or other sensitive information to evaluate and likely modify their current practices, including by implementing recurring in-depth assessments of such activities as further discussed below.

ADMT

While businesses utilizing artificial intelligence to process personal information may be relieved at the CPPA's lessened focus on artificial intelligence throughout the **drafting process** of the Regulations, such businesses may not be completely free and clear of the Regulations. ADMT is defined in the Regulations as "any technology that processes personal information and uses computation to replace human decision-making or substantially replace human decision-making." Accordingly, a business's use of artificial intelligence could fall under the umbrella of ADMT as the focus is not on the technology, but the human involvement in the decision-making process. Artificial intelligence and other technologies can assist humans in making decisions without being subject to the Regulations. It is only when human decision-making is substantially or totally replaced that the use of technology is considered ADMT.

The Regulations are triggered when ADMT is used by a business "to make a significant decision concerning a consumer" (**§7150; §7200(a)**). As early as January 1, 2027, such businesses must also provide to consumers (a) a pre-use notice describing in layman's terms the use of ADMT by the business and explaining the right of the consumer to opt-out of, and access, ADMT (**§7220**); (b) at least two easy methods "to opt-out of the use of ADMT to make a significant decision concerning the consumer" (subject to exceptions and opt-out denial rights) (**§7221**); and (c) easy-to-understand, specific explanations of how and why the business uses ADMT, including how ADMT was used to make a decision about that particular consumer, in response to a consumer's request for such information (**§7222**).

Risk Assessments

In addition to offering information and options regarding ADMT to consumers, certain businesses, as early as December 31, 2027, will also need to better understand such business's personal information processing activities and evaluate whether the risks of such processing activities and potential negative impact on consumers outweigh the benefits. Note that the benefits apply more broadly than to those enjoyed by the business, but also to stakeholders, consumers, and the public as a whole (**§7152**). The Regulations mandate that risk assessments include such details as: (a) the purpose of the processing; (b) a categorization of the to-be-processed personal information; (c) descriptions of certain aspects of the processing operations; (d) the benefits and potential negative impacts of the processing activities; and (e) planned safeguards the business intends to implement to address any such negative impacts.

Whether a business is required to conduct a risk assessment is dependent on certain activities conducted by such business. Such businesses will need to ask themselves the following questions:

- Does the business sell or share any personal information?
- Does the business process any *sensitive* personal information?
- Does the business use ADMT to make any "significant decision concerning a consumer"?
- Does the business conduct any automated processing based upon "systemic observation of that consumer" or upon "that consumer's presence in a sensitive location" to reach a particular judgement concerning a consumer, such as the intelligence, personal preferences, health, or reliability of that

consumer?
- Does the business intend to use consumers' personal information to train ADMT to render a "significant decision concerning a consumer"?

Affirmative answers to the above questions likely mean that such business, before beginning consumer personal information processing activities and at least once every three years thereafter (**§7155**), will need to conduct a risk assessment in accordance with the Regulations (**§7150**) and maintain records of each risk assessment for no less than five years after the applicable risk assessment is completed (**§7155**).

Cybersecurity Audits

Covered businesses will soon be required to conduct a cybersecurity audit if that business's consumer personal information processing activities present a "significant risk to consumers' security." The Regulations specify certain risk thresholds for businesses to consider, with metrics pointing to a business's revenue and the level of such business's processing activities (**§7120**).

Covered businesses may need to conduct their first audit as early as April 1, 2028, but no later than April 1, 2030, depending on the gross revenue of the business (**§7121**). Each cybersecurity audit must be conducted by an internal or external auditor who has "knowledge of cybersecurity and how to audit a business's cybersecurity program" and who is "objective and impartial" (**§7122**). To ensure an auditor's continued independence, businesses engaging internal auditors must conform to particular reporting structures as set forth in the Regulations (**§7122(a)(3)**).

To support such audits, businesses must provide to the auditor all requested information and relevant facts, and must not include misrepresentations (**§7122(b)-(c)**). Additionally, all audit findings must not be based primarily on the business's word, but on specific, actual evidence (**§7122(d)**).

The scope of the required cybersecurity audit is fairly broad, and essentially covers all handling, loss, use, and protection of personal information. Each cybersecurity audit also must evaluate whether the business's cybersecurity program is appropriate for the business (**§7123**). Such auditor then must issue a detailed report of their findings. Following the completion of an audit, both the auditor and the covered business must keep audit documents for at least five years following the applicable audit (**§7122**). Additionally covered businesses must certify to the CPPA that such business has completed the required cybersecurity audit every year the business is subject to such an audit.

Takeaway

We can expect new laws and requirements regarding ADMT and processing of personal information to continue popping up across the United States. While the scope of the applicability, restrictions, and requirements may vary, businesses should take time to develop a comprehensive understanding of their processing activities, including the reasons for and impacts of such, as well as update, or develop and implement, cybersecurity procedures and policies tailored to the business's activities. Your **Mintz Privacy and Security team** is ready to assist you with compliance with these new regulations and risk assessments.

Authors

M. Bertie Magit, Associate

M. Bertie Magit is an Associate at Mintz who focuses on commercial and licensing transactions such as intellectual property license and assignment agreements, research and development agreements, collaboration and option agreements, sponsorship agreements, influencer agreements, and other routine business transactions. Her clients include businesses of all sizes, including emerging companies.

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.