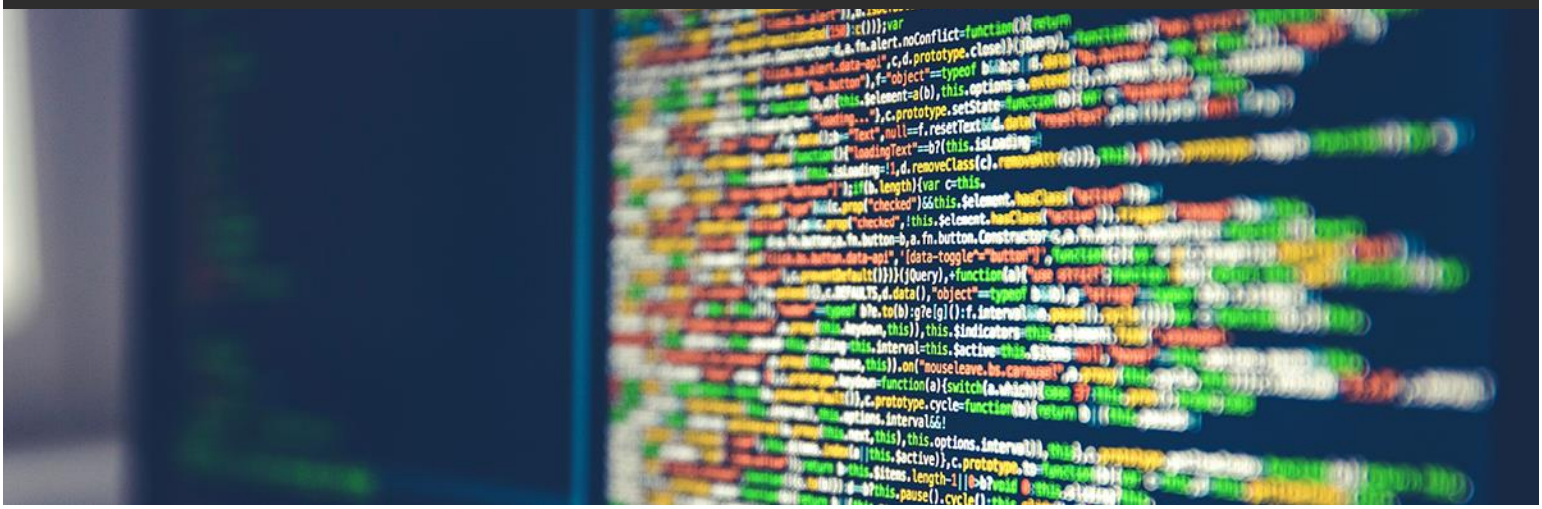
GT GreenbergTraurig

Alert | Data Privacy & Cybersecurity



September 2025

Revised and New CCPA Regulations Set to Take Effect on Jan. 1, 2026 – Summary of Near-Term Action Items

On Sept. 23, 2025, the California Privacy Protection Agency (CPPA) announced that the state's Office of Administrative Law (OAL) had formally approved the CPPA's wide-ranging package of revised and new California Consumer Privacy Act (CCPA) regulations, thereby confirming a Jan. 1, 2026, effective date.

Although the new rules do not contain a delayed enforcement grace period, as some earlier versions of the CCPA statute or amending rules had done, the new requirements pertaining to cybersecurity audits, risk assessments, and automated decision-making technology (ADMT) largely have compliance deadlines kicking in after the rules' 2026 effective date.

As highlighted below, many of the new provisions taking effect on New Year's Day – such as those pertaining to privacy policy disclosures, a business displaying on its website that it has processed a Global Privacy Control opt-out request, unsymmetrical dark pattern practices, and consent in relation to website cookie banners – are public-facing and may require near-term changes to companies' websites, mobile applications, or policies made available to consumers.

An overview of the main changes are addressed below but, given the nuance and detail contained within each, Greenberg Traurig's Data Privacy & Cybersecurity team will be monitoring the new cybersecurity audit, risk assessment, ADMT rules, and more. What follows below is an overview of some of the key changes taking effect Jan. 1, followed by the major takeaways for the new audit, assessment, and ADMT rules with later compliance deadlines.

CCPA Updates Effective Jan. 1, 2026

Displaying Confirmation of an Honored Opt-Out Request, Including GPC Signals

In-scope businesses going forward must provide a means for a California consumer to confirm that their request to opt-out of the selling/sharing of their personal information (PI) to third parties has been processed by the business, including in relation to receipt of opt-out preference signals such as the Global Privacy Control (GPC) technical standard. Whereas this was a discretionary provision before, such that a business could choose whether or not to confirm processing of an opt-out request and display such confirmation, it becomes a mandatory requirement starting next year.

The CPPA included as an example that this may be effectuated by displaying on a website, "Opt-Out Request Honored," and using a toggle or radio button in the consumer's privacy settings to indicate whether the consumer has opted out, but the reference in the rules to "for example" suggests that other compliant implementations may be possible. This new rule is particularly relevant given the CPPA's recent announcement on Sept. 9 of a joint investigative sweep with the Colorado and Connecticut attorneys general in relation to businesses' compliance with GPC opt-out requests.

Cookie Consent Banner Updates – 'X'ing' Out Does Not Mark the Opt-In Consent Spot

The updated rules clarify that a "consumer closing or navigating away from a pop-up window on a website that requests consent without first affirmatively selecting the equivalent of an "I accept" button shall not constitute consent. Such a method for obtaining consent is confusing to the consumer."

This new requirement seems to effectively confirm that if using an opt-in approach to sell/share tracking technologies on a website (i.e., to seek to avoid the disclosure of such PI being treated as a sale/share, as the consumer "direct[ed] the business to intentionally disclose" the PI per CCPA Section 1798.140(ad)(2)(A), consent inferred from someone closing a cookie banner is not viewed by the CPPA as meaningful consent and could be considered a dark pattern. The rules also indicate that a choice where a "yes" button (e.g., for consent or opt-in) is more prominent (e.g., in size or color) than a "no" button will not be viewed as equal or symmetrical.

Symmetry in the Opt-Out Process – Equal Number of Steps to Opt-Out as to Opt-In

As an update to the CCPA regulations' design and consent requirements, the new rules affirm that the number of steps a consumer must take to request to opt-out of the sale or sharing of their PI – as measured from when the consumer clicks on a "Do Not Sell or Share My Personal Information" link to completion of the request – should be "the same or fewer" than the number of steps for submitting a request to opt-in to the sale/sharing of PI, where the business offers a link to consumers to learn more about opting-in to such selling/sharing. Failure to do so, the rules confirm, is not symmetrical from a dark patterns standpoint. Companies should consider this in relation to their potential selling/sharing cookie consent practices as well.

Financial Incentive Programs May Not Be Selected by Default

The new rules hold that it is also not symmetrical to select a consumer's participation in a financial incentive program by default or to feature an opt-in to such a program more prominently than the choice not to participate in it.

New Mechanisms for Requests to Know Looking Back to Jan. 1, 2022

The new rules establish that if a business maintains the PI of a consumer for longer than 12 months, its consumer request mechanism(s) must include a means by which the consumer can request access to PI collected *prior* to the 12-month period preceding the consumer's request. The CPPA included as an example that a business "may ask the consumer to select or input the date range for which the consumer is making the request to know or present the consumer with an option to request all [PI] the business has collected about the consumer" going back to Jan. 1, 2022.

Privacy Policy Updates – Required Identification of PI Categories Disclosed to a Service Provider

Whereas currently under the CCPA businesses are required to identify in their privacy policies any categories of PI disclosed to third parties, the revised rules remove any ambiguity and confirm that the privacy policy must also identify any categories of PI disclosed to a service provider or contractor for a business purpose in the preceding 12 months.

Mobile Applications Must Include a Link to the Privacy Policy in the Application's Settings Menu

Whereas currently a mobile application "may" include a link to the privacy policy in the application's settings menu, the revised rules clarify that a mobile application instead "must" do so. This might prompt updates for those mobile app-offering companies not currently doing so.

New Rules for Timing of Opt-Out Notices in Relation to IoT/Connected Devices, AR/VR

As an extension of the current requirement to provide a notice of a consumer's right to opt-out in the same manner in which the business collects the PI that it sells or shares, the new rules establish that for PI sold/shared through a connected device, such as a smart television or a smart watch, the business must provide the opt-out notice "before or at the time the device begins collecting the PI" to be sold/shared. In its Final Statement of Reasons regarding the CCPA rule updates, the CPPA opined that this rule change "benefits businesses by providing flexibility in how to provide the various notices required under the statute and allowing them to use one notice to meet both the notice at collection and notice of right to opt-out of sale/sharing requirements."

Similarly, if a business sells PI collected in an augmented reality (AR) or virtual reality (VR) setting, "such as through gaming devices or mobile applications," the business must now provide the opt-out notice either (1) before or at the time the consumer enters the AR/VR environment, or (2) before or at the time the consumer "encounters the business within the" AR/VR environment. No further description of what it means to "encounter a business" is provided.

Clarification of Partial Exemption Limited to Data Governed by the State Insurance Code

The new rules define an "insurance company" as any person subject to the California Insurance Code, including insurance institutions, agents, and insurance-support organizations. The regulations confirm that in-scope insurance company businesses are required to comply with the CCPA in relation to any PI not subject to the Insurance Code, such as for PI not collected in connection with an insurance transaction or for provision of a financial product or service (e.g., marketing website data or employee/job applicant data).

New Rules Primarily Taking Effect After 2026

Automated Decision-Making Technology – New Notice, Opt-Out, and Access Request Requirements

The rules confirm that a business that uses automated decision-making technology (ADMT) for a significant decision prior to Jan. 1, 2027, must comply with the ADMT requirements by that date. Any such ADMT use after the start of 2027 must comply with the relevant rules prior to being implemented.

Omitting any reference to "artificial intelligence," the updated rules contain the newly defined term, "automated decision-making technology." This refers to any technology that processes PI and uses computation to replace or "substantially replace human decision-making" – the latter itself being a defined term that is described as when a business uses technology to make a decision without "human involvement," which is also defined.

When a business uses ADMT to make a "significant decision" about a California consumer in relation to financial or lending services, housing, educational opportunity/enrollment, employment/compensation, or health care services, new obligations will apply. Notably, the final rules clarify that advertising to a consumer does not, by itself, constitute a significant decision.

The ADMT rules will require the following (and more):

- Provision of a conspicuous "Pre-use Notice" informing consumers about the business's specific purpose for using ADMT;
- A description of the rights to opt out of ADMT and request access to information about the business's use of ADMT to make a significant decision, and how to make such requests;
- Additional information about "how the ADMT works to make a significant decision about consumers, and how the significant decision would be made if a consumer opts out," while also providing information about the type of output the ADMT generates; and
- A description of what the alternative process for making a significant decision is for consumers who opt out.

Privacy Risk Assessments and the Requirement to Submit Summaries to the CPPA Annually Starting April 1, 2028

When processing of PI presents "significant risk" to consumers' privacy a business must conduct a risk assessment before initiating such PI processing. The new risk assessment requirement applies to the activities listed below that a business initiated prior to 2026, and that continues into 2026, and requires a business to complete the risk assessment no later than Dec. 31, 2027. The new rules identify the following activities as presenting significant risk:

- Selling or sharing (i.e., for cross-contextual behavioral advertising) PI;
- Processing sensitive PI;
- Using ADMT for a significant decision concerning a consumer;
- Processing PI to train ADMT for a significant decision concerning a consumer, or to train facial/emotional recognition or other identity verification technology or profiling of a California consumer;

- Using automated processing to infer or extrapolate information about an employee, job applicant, contractor or student's intelligence, ability, work performance, economic situation, health, personal preferences, interests, behavior, location or movements, based on a systemic observation of that consumer; and/or
- Using automated processing to infer or extrapolate the same based on a person's presence in a "sensitive location," defined as healthcare facilities including hospitals, doctors' offices, urgent care facilities, and community health clinics; pharmacies; domestic violence shelters; food pantries; housing/emergency shelters; educational institutions; political party offices; legal services offices; union offices; and places of worship.

Unlike other state privacy laws requiring risk assessments, under the new rules, businesses are required to submit a summary report annually on April 1, containing certain risk assessment details, such as the number of risk assessments conducted or updated, whether they involved sensitive data, and include an attestation signed by a sufficiently knowledgeable and directly responsible "member of the business's executive management team…under penalty of perjury under the laws of the state of California." The first summary report of risk assessments of 2026 and 2027 activities must be submitted by April 1, 2028. And while businesses are only required to submit a summary report, the CPPA or Attorney General of California may at any time request copies of a business's risk assessment reports, which businesses must produce within 30 calendar days of such a request.

As a reminder, a key distinction between risk assessments for California compliance compared to privacy-related risk assessments required by other U.S. states is that the CCPA applies to personal information collected in an employment/HR-related context (e.g., former/current employees, job applicants and contractors) and in a business-to-business (B2B) context. Thus, while risk assessments prepared for other jurisdictions may be leveraged, job applicant, employee and B2B data will need to be considered as well for CCPA compliance.

Cybersecurity Audits – Detailed Reviews Conducted Against an 18-Point List

The new rules, which become effective from 2028 to 2030 based on a business's annual gross revenue for a given preceding year (e.g., more than $100 million or more or less than $50 million), hold that any business whose processing of Californians' PI presents "significant risk" to consumers' security must complete a cybersecurity audit. In this context, significant risk is present if a business, in the preceding calendar year:

- Earned 50% or more of its gross global revenue from selling or sharing PI; or
- Had $26.625 million in gross global revenue and processed either (1) the PI of 250,000 or more consumers/households, or (2) the sensitive PI of 50,000 or more consumers.

The new rules require use of an internal or external auditor subject to certain qualifications; findings may not "rely primarily on assertions or attestations by the business's management" but rather must be based on "specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted)" as the auditor sees fit; and a written certification must be submitted to the CPPA in April following the year a cybersecurity audit was required to be completed, summarizing certain audit information and having to be signed by a member of the business's executive management team under penalty of perjury.

Audits must cover 18 components of a cybersecurity program, as identified in the rules, ranging from network segmentation to oversight of service providers and contractors, to use of multifactor

authentication, to security incident response processes, to cybersecurity training and log monitoring, among others.

These new requirements may be somewhat familiar to companies subject to Securities and Exchange Commission cybersecurity risk management disclosures or New York Department of Financial Services cybersecurity regulation filing requirements, for instance, but they may represent new areas of attention for many companies not already subject to such regulatory standards.

Authors

This GT Alert was prepared by:

- Darren J. Abernethy | +1 415.655.1261 | abernethyd@gtlaw.com
- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com