ISSUE BRIEF

US POLICY

CCPA Regulations on Automated Decisionmaking Technology, Risk Assessments, and Cybersecurity Audits

October 2025

Jordan Francis, Senior Policy Counsel, U.S. Legislation
Justine Gluck, Policy Analyst, AI Policy and Legislation

FUTURE OF PRIVACY FORUM

Executive Summary

Since the California Consumer Privacy Act (CCPA) was enacted in 2018, business obligations under the law have continued to evolve due to several rounds of rulemaking by both the Attorney General and the California Privacy Protection Agency (CPPA). The latest regulations from the CPPA—finalized in September 2025—are some of the most significant yet. Starting January 1, 2026, businesses will be subject to extensive new obligations concerning automated decisionmaking technology (ADMT), risk assessments, and cybersecurity audits. This issue brief analyzes these new regulations with a focus on potential compliance challenges and how these requirements compare to other state privacy laws. Some key takeaways include:

1. **Businesses using ADMT to make significant decisions about consumers must—**
    a. Provide pre-use notice to consumers, and
    b. Comply with consumer requests to opt-out of the use of ADMT and to access information about the business's ADMT use;
2. **Businesses whose processing of personal information presents significant risk to consumers' privacy must—**
    a. Conduct a risk assessment before initiating the high-risk activity,
    b. Regularly submit information about conducted risk assessments to the CPPA, and
    c. Disclose completed risk assessment reports to the Attorney General or the CPPA upon demand; and
3. **Businesses whose processing of personal information presents significant risk to consumers' security must—**
    a. Conduct an annual cybersecurity audit, and
    b. A qualified member of the business's executive management team must submit a written attestation that an audit has been conducted.

Acknowledgements

The authors thank Beth Do and Tatiana Rice for their contributions to this issue brief.

Table of Contents

Introduction

Businesses' obligations under the California Consumer Privacy Act (CCPA) continue to evolve. Starting on January 1, 2026, CCPA-regulated businesses will be subject to extensive new obligations concerning automated decisionmaking technology, risk assessments, and cybersecurity audits. This new rulemaking package is merely the latest milestone in the CCPA's ever-evolving regulatory landscape. The California Attorney General finalized an initial set of CCPA regulations in 2020 before passing amendments in 2021.[1] Following the enactment of Proposition 24, rulemaking authority was transferred to the newly created California Privacy Protection Agency (CPPA) in 2022.[2] Since then, the CPPA has completed two major rulemaking packages under the CCPA, as well as extensive rulemaking under the Delete Act.[3]

The below timeline shows extensive, iterative rulemaking under the law, with the effective date for the new regulations coming into effect January 1, 2026, providing a short window for businesses to build out compliance programs.[4]

CCPA Regulatory Timeline: 2018 to Present	
June 28, 2018	AB 375, the California Consumer Privacy Act (CCPA), is signed into law
January 1, 2020	CCPA becomes effective
August 14, 2020	Initial CCPA regulations become effective
November 3, 2020	Proposition 24, the California Privacy Rights Act (CPRA), is enacted
March 15, 2021	Additional CCPA regulations become effective
April 21, 2022	Rulemaking authority is transferred to the new California Privacy Protection Agency (CPPA)
July 8, 2022	Public notice of rulemaking pursuant to the CPRA
March 27, 2023	Preliminary comments close for proposed rulemaking on cybersecurity audits, risk assessments and automated decisionmaking technology

[1] Cal. Dep't of Justice, *CCPA Regulations*, https://oag.ca.gov/privacy/ccpa/regs (last visited Aug. 19, 2025).
[2] The agency's official name is the California Privacy Protection Agency (CPPA). In September 2025, the Agency voted to rebrand its abbreviation as "CalPrivacy." Tyler Katzenberger, *CPPA Embraces New Nickname: 'CalPrivacy,'* Politico Pro (Sept. 26, 2025), https://subscriber.politicopro.com/article/2025/09/cppa-embraces-new-nickname-calprivacy-00583288.
[3] Cal. Priv. Prot. Agency, *Laws & Regulations*, https://cppa.ca.gov/regulations (last visited Oct. 6, 2025).
[4] Note that some of the new obligations are staggered. For example, cybersecurity audits will not be required to be completed until April 1, 2028 at the earliest. *Infra* Part III.C.

March 29, 2023	Initial CPRA regulations are finalized and become effective immediately[5]
November 22, 2024	Public notice of rulemaking on CCPA updates, cybersecurity audits, risk assessments, ADMT, and insurance companies
July 24, 2025	CPPA Board votes to adopt proposed regulations
January 1, 2026	New regulations on CCPA updates, cybersecurity audits, risk assessments, ADMT, and insurance companies will become effective

This issue brief analyzes these new regulations with a focus on potential compliance challenges and how these requirements compare to other state privacy laws. All in-line citations are to the updated CCPA regulations, as found in California Code of Regulations, title 11, division 6.

I. Automated Decisionmaking Technology Access and Opt-out Rights

Much of the attention on this latest rulemaking package has been directed at the automated decisionmaking technology (ADMT) regulations, which require covered businesses to conduct certain governance practices and provide new consumer rights when using ADMT to make significant decisions concerning consumers. This section explores:

- The **scope** of the ADMT regulations, identifying the degree to which an automated system must play a role in the decisionmaking process, the extent "profiling" constitutes ADMT, and the scope of covered decisions;
- The **additional governance requirements** include providing pre-use notices, conducting risk assessments, and compiling metrics on the use of ADMT and consumer rights; and
- **Consumer rights** to (1) opt-out of a business' use of ADMT with respect to them, and (2) obtain information from the business about the business's use of ADMT with respect to them.

A. Scope

The ADMT regulations apply to any "business that uses ADMT to make a significant decision concerning a consumer." (§ 7200.) "Business" is an established term under the CCPA, but "ADMT" and "significant decision" are novel terms. To determine whether these regulations apply, businesses must evaluate (1) whether they are using automated decisionmaking for significant decisions (e.g., financial or lending services, housing, education, employment, or healthcare), (2) whether their use of automated decisionmaking in that context meets the definition of ADMT (i.e., replaces or substantially replaces human decisionmaking), and (3) if any exemptions apply.

[5] The initial CPRA regulations were subject to litigation concerning their effective date. Ultimately, the California Court of Appeals ruled that the new regulations could be enforced immediately rather than one-year after finalization. Cal. Priv. Prot. Agency v. Superior Court, 318 Cal. Rptr. 3d 90 (Cal. Ct. App. 2024).

1. Significant Decisions

The ADMT regulations apply when a business uses an ADMT that replaces or substantially replaces human decisionmaking to make ***"a significant decision concerning a consumer."*** (§ 7200, subsec. (a).) The term "significant decision," in turn, 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." (§ 7001, subsec. (ddd).) Those five categories are defined in greater detail:

Financial or Lending Services: "[T]he extension of credit or a loan, transmitting or exchanging funds, the provision of deposit or checking accounts, check cashing, or installment payment plans."

Housing: "[A]ny building, structure, or portion thereof that is used or occupied as, or designed, arranged, or intended to be used or occupied as, a home, residence, or sleeping place by one or more consumers including for permanent or temporary occupancy. *The use of 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.*" (emphasis added)

Education Enrollment or Opportunities: "(A) Admission or acceptance into academic or vocational programs; (B) Educational credentials (e.g., a degree, diploma, or certificate); and (C) Suspension and expulsion."

Employment or Independent Contracting Opportunities or Compensation: "(A) Hiring; (B) Allocation or assignment of work for employees; or salary, hourly or per-assignment compensation, incentive compensation such as a bonus, or another benefit . . . ; (C) Promotion; and (D) Demotion, suspension, and termination."

Healthcare Services: "[S}ervices related to the diagnosis, prevention, or treatment of human disease or impairment, or the assessment or care of an individual's health."

Apart from the categories of decisions subject to regulation, scoping is also determined by the finality of decisions that are in scope. The CCPA regulations concern the ***"provision or denial"*** of listed goods and services. That language is narrower than earlier drafts that referred to "access to" goods and services, which risked incorporating tangential use cases or intermediate decisions. For example, a navigation app directing someone to a hospital could have been considered "access to" healthcare services. By contrast, under the final rules, ADMT is only implicated when the system directly determines whether a service is ***provided or denied***.

The Regulations' "Significant Decision" Framework Is Similar to Other Laws' Approach: The "significant decisions" framework fits into a broader legislative trend, both in U.S. state law and

globally.[6] Article 22 of the General Data Protection Regulation (GDPR) provides a right for data subjects "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[7] U.S. state laws adapted that language but provide additional specificity. State comprehensive privacy laws, for example, often provide opt-out rights with respect to profiling in furtherance of decisions that result in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.[8] The Colorado AI Act similarly applies to "consequential decisions," but it also reaches further by covering essential government services, insurance, and legal services—three areas not included under the CCPA's regulations. Thus an ADMT tool used for insurance underwriting could be regulated under Colorado's law, but not under California's CCPA rules. Businesses operating across states may need to be aware of these distinctions.

Advertising and the Scope of ADMT Requirements: The regulations are explicit that "significant decision" ***does not*** include advertising to a consumer. (§ 7001, subsec. (ddd)(6).) This was unclear in prior drafts, as they would have expanded the definition of "significant decision" to include decisions that result in "access to" the covered goods and services; that language was removed from the final draft. Processing personal information for advertising remains regulated under the CCPA generally, as businesses must still comply with existing requirements such as the right to opt-out of the sale or sharing of personal information for cross-context behavioral advertising. However, the regulations do not add heightened ADMT access or opt-out rights for advertising.

2. Defining ADMT

The final CCPA regulations define "automated decisionmaking technology" (ADMT) as technology that processes personal information and uses computation to ***"replace"*** or ***"substantially replace"*** human decisionmaking. (§ 7001, subsec. (e).)

The regulations further clarify that a technology "substantially replace[s] human decisionmaking" if the business "uses the technology's output to make a decision without human involvement." (§ 7001, subsec. (e)(1).) For a decision to qualify as involving human involvement, the human reviewer must:

A. Know how to interpret and use the technology's output to make the decision;

---

[6] Tatiana Rice, Jordan Francis & Keir Lamont, U.S. State AI Legislation: How U.S. State Policymakers Are Approaching Artificial Intelligence Regulation 5–6, (Sept. 2024), https://fpf.org/wp-content/uploads/2024/09/FINAL-State-AI-Legislation-Report-webpage.pdf; Justine Gluck, Beth Do & Tatiana Rice, The State of State AI: Legislative Approaches to AI in 2025, at 7, FPF (Oct. 2025), https://fpf.org/wp-content/uploads/2025/10/The-State-of-State-AI-2025.pdf.

[7] GDPR, art. 22.

[8] Jordan Francis, Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends at 11, fn. 28 (Nov. 2024), https://papers.ssrn.com/id=5309115.

B. Review and analyze the output of the technology, and any other information that is relevant to make or change the decision; and

C. Have the authority to make or change this decision (§ 7001, subsec. (e)(1).)

Under these standards, the regulations appear to set a relatively high bar for "human involvement," requiring the human to actively analyze the decision and retain ultimate authority. Businesses will need to evaluate whether their current review processes meet requirements and whether their "human in the loop" functions are sufficient to meet the standard. For instance, compliance questions may be raised for companies that rely on automated scoring systems with limited human oversight (e.g., credit scoring or hiring algorithms).

Narrowed Rules Illustrate Difficulties in Scoping AI Regulation: Over the course of the multi-year rulemaking process, the scope of the proposed ADMT regulations narrowed. Earlier iterations of these rules were much broader, extending not only to ADMT but also to "artificial intelligence," which was separately defined. This framing would have brought a wider range of technologies within scope. Following criticism that the agency was exceeding its statutory authority, references to "artificial intelligence" were removed and the regulations were refocused exclusively on ADMT.[9]

The final rules are also narrower in how they define ADMT. While early drafts included technologies that "substantially facilitate" human decisionmaking, the final language applies only when ADMT "substantially replaces" human decisionmaking. The CCPA regulations therefore are only triggered when the human role is essentially removed or rudimentary (i.e., when use of the technology largely drives the decision). Other automated decisionmaking regulations take a broader approach. Recently enacted regulations from the California Civil Rights Council (CCRC) addressing the role of automated-decision systems (ADS) in employment settings under the Fair Employment and Housing Act (FEHA), for example, apply even when a human makes the final call as long as the ADS influences or supports (i.e., facilitates) that decision.[10] This distinction may make the FEHA regulations significantly broader in practice than the CCPA regulations.

This debate around when ADMT "facilitates" as opposed to "replaces" human decisionmaking underscored concerns about the types of technologies within the CCPA's scope. A "facilitates" standard could inadvertently capture basic tools such as calculators or spreadsheets that do not warrant regulation. This concern was mitigated when the Agency swapped "substantially facilitate" with "substantially replace" and added an explicit carve-out for specific technologies. ADMT does not include "web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, and spreadsheets." However, the exception itself has an exception: Those

[9] In responses to comments on the draft regulations, the Agency disagreed with claims that it was exceeding its statutory mandate. *See, e.g.*, FSOR Appendix A, at 2, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_fsor_appen_a.pdf.
[10] Cal. Code Regs., tit. 2, § 1108.1, subsec. (a).

technologies are only exempted so long as "they do not replace human decisionmaking." (§ 7001, subsec. (e)(3).)

3. Profiling and Systematic Observation

The CCPA regulations further specify that ADMT includes "profiling that replaces human decisionmaking or substantially replaces human decisionmaking." Profiling is defined as "automated processing of personal information to evaluate certain aspects . . . relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior, location, or movements." The "aspects" of a person evaluated via profiling include "intelligence, ability, aptitude, [and] predispositions." Note that this is written as ***"including"*** those aspects, which suggests an open standard. (§ 7001, subsec. (ii).)

Ultimately, "profiling" may have little to no significance under the regulations on its own. The term appears few times in the regulations and mostly only as a nested definition within the terms "ADMT," "physical or biological identification or profiling," and "systematic observation."[11] Those latter two terms are relevant to risk assessment requirements.[12]

ADMT: "ADMT includes ***profiling*** that replaces human decisionmaking or substantially replaces human decisionmaking."

Physical or biological identification or profiling: "[I]dentifying or ***profiling*** a consumer using automated measurements or analysis of their physical or biological characteristics, or automated measurements or analysis of or relating to their body. This includes using biometric information, vocal intonation, facial expression, and gesture (e.g., to identify or infer emotion). This does not include processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer."

Systematic Observation: "[M]ethodical and regular or continuous observation. This includes, for example, methodical and regular or continuous observation using Wi-Fi or Bluetooth tracking, radio frequency identification, drones, video or audio recording or live-streaming, technologies that enable ***physical or biological identification or profiling***; and geofencing, location trackers, or license-plate recognition."

The regulations do not include standalone requirements for profiling. Nevertheless, the definition of profiling may provide additional illustrative examples of business practices and technologies that may trigger ADMT obligations, at least when profiling is used to make a significant decision and replaces or substantially replaces human decisionmaking. Among the categories in the definition of profiling, "performance at work" is especially relevant for businesses' AI governance in the workplace. The regulations clarify that "performance at work" refers specifically to "the

[11] Profiling also appears in one of the examples of negative economic harm to consider in conducting a risk assessment: "compensating consumers at lower rates based upon profiling." § 7152, subsec. (a)(5).
[12] *Infra* Part II.

performance of job duties for which the consumer has been hired or has applied." It does not extend to activities outside that scope, such as union membership, a consumer's off-duty location, interest in seeking other employment, or use of a personal account. This definition of profiling brings many common workplace and consumer-facing technologies within scope, such as employee monitoring tools, productivity scoring, or behavioral tracking technologies.

Evaluating "personal preferences" is another profiling purpose that could capture the use of commonplace technologies, such as dynamic pricing algorithms that process personal information.[13] However, such profiling purposes must still trigger one of the regulations obligations with respect to using ADMT to make a significant decision, physical or biological identification or profiling, or systematic observation.

B. Business Obligations Prior to ADMT Use

The regulations impose robust obligations on businesses in addition to the new consumer rights: Covered entities must provide pre-use notices, conduct risk assessments, and compile metrics on use of ADMT access and opt-out rights.

The most substantial obligation for businesses ***prior to ADMT use*** is to provide consumers with a pre-use notice informing them about the business's use of ADMT and their right to opt-out of ADMT and right to access ADMT. (§ 7010, subsec. (c).) The pre-use notice must be presented to the consumer "at or before" the point when the business ***collects*** the consumer's personal information to be used with ADMT. If the information has already been collected to be used for a different purpose, and the business now plans to process it using AMDT, a pre-use notice must still be provided before that processing occurs. The notice must also be presented "prominently and conspicuously" and delivered in the manner in which the business primarily interacts with the consumer.

Prior drafts of the regulations would have required that notice be provided "upon processing" rather than "upon collection." This shift in timing poses compliance considerations. Businesses must anticipate potential ADMT uses at the time of data collection, not later in the data lifecycle. In practice, businesses that collect large volumes of consumer data but only decide to apply ADMT at a later stage may find themselves out of compliance if pre-use notices were not properly issued at collection. The regulations account for this by allowing for pre-use notice for a secondary purpose before that processing occurs. While this provides some flexibility, it still requires businesses to revisit processes, re-engage consumers with new disclosures, and establish clear procedures for tracking when data shifts into ADMT-related use.

[13] *See generally* Jameson Spivack, *Data-Driven Pricing: Key Technologies, Business Practices, and Policy Implications*, FPF (July 14, 2025), https://fpf.org/resource/data-driven-pricing-key-technologies-business-practices-and-policy-implications.

Pre-use notices include the following:

1. A plain language description of the ***specific purpose*** for which the business plans to use the ADMT, which ***cannot be described in generic terms***;
2. A Description of the consumer's ***right to opt-out*** of ADMT and how they can submit an opt-out request, unless
    A. If the business is relying on the ***"human appeal exception,"*** the business must inform the consumer of their ability to appeal the decision and instructions on how to submit the appeal, or
    B. If the business is relying upon another exception to the opt-out right, it must identify that specific exception;
3. Description of the consumer's ***right to access*** ADMT and how the consumer can submit their request to access ADMT;
4. That a business cannot retaliate against consumers for exercising their CCPA rights;
5. Additional information about how the ADMT makes a significant decision and how the significant decision would be made after a consumer opts-out. This information may be provided "via a simple and easy-to-use method" such as a hyperlink. The "additional information" must include a plain language description of the following:
    A. "How the ADMT processes personal information to make a significant decision about consumers, including the ***categories of personal information that affect the output generated by the AMDT***" (emphasis added);
    B. "The type of output generated by ADMT and how that output is used to make a significant decision," which "may include whether the output is the sole factor in the decisionmaking process or what the other factors are in that decisionmaking process," and "to the extent that a human is part of the decisionmaking process in a manner that does not meet the requirements of 'human involvement'"; and
    C. "What the alternative process for making a significant decision is for consumers who opt-out, unless an exception to providing the opt-out of ADMT . . . applies." (§ 7220, subsec. (c).)

These requirements mandate detailed, specific descriptions, connecting data use to a clearly defined decision-making function, rather than broad or "generic" justifications. For instance, the obligation to disclose the "categories of personal information" that affect outputs requires businesses to map data inputs and understand how those inputs influence outcomes. This may create compliance challenges for organizations using vendor-supplied "black box" systems that cannot be easily explained. Because businesses remain responsible for CCPA compliance even when using third-party ADMT tools, they may need to include contractual provisions requiring vendors to share sufficient technical detail to support disclosures. While the regulations do not directly impose these duties on vendors, they effectively increase pressure on service providers to provide documentation for these partnerships.

In efforts to ease compliance and protect important business interests, the regulations specify that the pre-use notice is not required to include trade secrets or information that would compromise the business's ability to prevent, detect, and investigate security incidents, resist malicious or illegal actions, prosecute those responsible for those actions, or ensure the physical safety of individuals. (§ 7220, subsec. (d).)

The regulations also provide that pre-use notices can be consolidated in the following contexts:

- If the business is using a single ADMT for multiple purposes (e.g., an employer providing a single notice to an employee about "the employer's proposed use of productivity monitoring software to determine the employee's allocation/assignment of work and compensation, ***and*** to determine which employees will be demoted");
- If a business is using multiple ADMTs for a single purpose (e.g., a business providing a single notice to a job applicant addressing the proposed use of "(1) software to screen applicants' resumes to determine which applicants it will hire, and (2) software to evaluate applicants' vocal intonation, facial expression, and gestures to determine which applicants to hire");
- If a business is using multiple ADMTs for multiple purposes (e.g., an educational provider could provide a single notice to a new student addressing the proposed use of "(A) software that automatically screens students' work for plagiarism to determine whether they will be suspended, and (B) software that automatically assesses students' exams to determine whether to grant them a diploma or certificate"); or
- If a business is making ***"systematic use"*** of a single ADMT (e.g., an employer can provide one notice to an employee addressing the employer's "methodical and regular use of ADMT to allocate work to its employees").(§ 7220, subsec. (e) (emphasis added).)

The consolidated pre-use notice must include all the information required under the regulations. The ability to issue a consolidated pre-use notice allows businesses to streamline disclosures across multiple ADMT systems or purposes, reducing administrative burdens and helping avoid "notice fatigue" for consumers while still advancing the regulations' transparency goals. At the same time, consolidation carries challenges: businesses must ensure that each ADMT use is accurately described, that disclosures remain clear and comprehensible, and that explanations are specific rather than "generic."

C. Consumer Rights

The updated regulations introduce two novel consumer rights under the CCPA: The "Right to opt-out of ADMT" and the "Right to access ADMT."

1. Requests to Opt-Out of ADMT

Under the regulations, a business must provide consumers with the ability to ***opt-out*** of the use of ADMT "to make a significant decision concerning the consumer." At least two designated

methods for submitting opt-out requests are required and at least one of those methods must reflect the way the business primarily interacts with the consumer. (§ 7221, subsec. (c).) For example, a business that engages with consumers both in person and online ***may*** provide both a physical form and an online form to submit opt-out requests. For businesses that interact with consumers online, one required option is an interactive form accessible through an opt-out link included in the pre-use notice. Other acceptable methods may include a toll-free phone number, a designated email address, an in-person form, or a mail-in form. (§ 7221, subsec. (c)(3).) The regulations clarify that cookie banners are not valid opt-out mechanisms, since cookies relate to data collection, not necessarily the use of ADMT. (§ 7221, subsec. (c)(4).)

Additional requirements for opt-out requests include:

- The method of submitting opt-out requests must be ***easy*** for consumers to execute and require ***minimal steps***;
- The business must not require a consumer to create an account or provide additional information beyond what is necessary;
- The business must ***not require a verifiable consumer request*** for a request to opt-out, and, to the extent that the business can comply with a request to opt-out of ADMT without additional information, it must do so;
- If a business has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request, but it must provide the requestor an explanation as to why;
- The business must provide a means by which the consumer can confirm that the business has processed their request to opt-out of ADMT;
- As long as the business provides a single option to opt-out of all the business's uses of ADMT, the business may present the consumer with the choice to allow specific use cases of ADMT in responding to an opt-out request;
- A consumer may use an authorized agent to submit an opt-out request, so long as the consumer provides the authorized agent signed permission;
- After a business receives an opt-out request, it must ***wait at least 12 months*** from that date before asking a consumer who has exercised their right to opt-out of ADMT to consent to the business's use of the ADMT;
- The business cannot retaliate against a consumer because the consumer exercised their opt-out right;
- The business must not initiate processing of the consumer's personal information using an ADMT if the consumer submits a request to opt-out of ADMT before the business has initiated that processing;
- If the consumer submitted a request to opt-out of ADMT after the business initiated the processing, the business must comply with the consumer's opt-out request by:

- Ceasing to process the consumer's personal information using that ADMT as soon as feasibly possible, but no later than ***15 business days*** from the date the business receives the request; and
- Instructing the business's service providers, and other persons to whom the business has made personal information for ADMT use available, to comply with the consumer's request to opt-out of that ADMT within the same time frame.

The business is not required to offer the ability to opt-out in the following circumstances:

- When the consumer has the ability to appeal the decision to a human reviewer who can overturn it (the ***"human appeal exception"***) In this case, the reviewer must understand and be able to interpret the ADMT output and have actual authority to change the decision. Businesses must describe the appeal process to the consumer and ensure it is easy to use.
- For admission, acceptance, or hiring decisions, when ADMT is used ***solely*** to assess a consumer's ability to perform at work or in an educational program to determine whether to admit, accept, or hire them, provided that the use of ADMT does not unlawfully discriminate based upon protected characteristics.
- For work allocation and compensation decisions, when ADMT is used ***solely*** to allocate or assign work or compensation and the ADMT does not unlawfully discriminate based upon protected characteristics.

To meet these opt-out requirements, businesses will need to invest in consumer-facing processes that are clear and accessible across multiple channels. For companies with large-scale ADMT use, ensuring that opt-out requests are transmitted to all service providers within 15 business days may require new systems. The exemptions are also notable: they allow businesses to continue using ADMT in key functions like hiring or work allocation, provided there is a nondiscriminatory purpose and a meaningful human appeal process. For compliance, this means companies must not only document why their use falls within an exemption, but also demonstrate that human reviewers are trained and available to overturn decisions when necessary. However, the regulations do not specify qualification standards for human reviewers, such as the scope of "authority to change the decision based on their analysis." As a result, questions remain about how businesses can ensure their appeal processes fully satisfy exemption requirements.

2. Requests to Access ADMT

In addition to other transparency requirements, such as mandated pre-use notices, consumers also have the right to access information about a business's use of ADMT to make a significant decision concerning the consumer. (§ 7222, subsec. (a).) If a consumer submits an access request, the business must provide plain-language explanations of the following:

1. The ***specific purpose*** for which ADMT was used with respect to the consumer, described in non-generic terms;

2. Information about the ***logic of the ADMT*** that enables the consumer to understand how their personal information was processed to generate an output, which may include parameters and specific outputs;
3. The ***outcome of the decision-making process***, including how ADMT was used to reach the decision (e.g., whether the output was the sole factor, what other factors were considered, and the role of any human involvement) and how the business plans to use that output to make a significant decision about the consumer in the future; and
4. That the business is ***prohibited from retaliating*** against consumers for exercising their CCPA rights and offering instructions for how the consumer can exercise their other CCPA rights (which may be satisfied through a direct link to the relevant section of the business's privacy policy). (§ 7222, subsec. (b).)

Like pre-use notices, access request responses are not required to include trade secrets or information that could compromise security, fraud prevention, or physical safety. (§ 7222, subsec. (c).) However, other requirements include:

- Submission methods must be easy to use and free from ***dark patterns***;
- ***Verification requirements apply***, but, if a verified request is denied, then the business must notify the consumer and explain the basis for denial;
- Businesses must use reasonable security measures when transmitting requested information and may use secure portals; and
- Service providers and contractors must assist businesses in responding to verified requests.

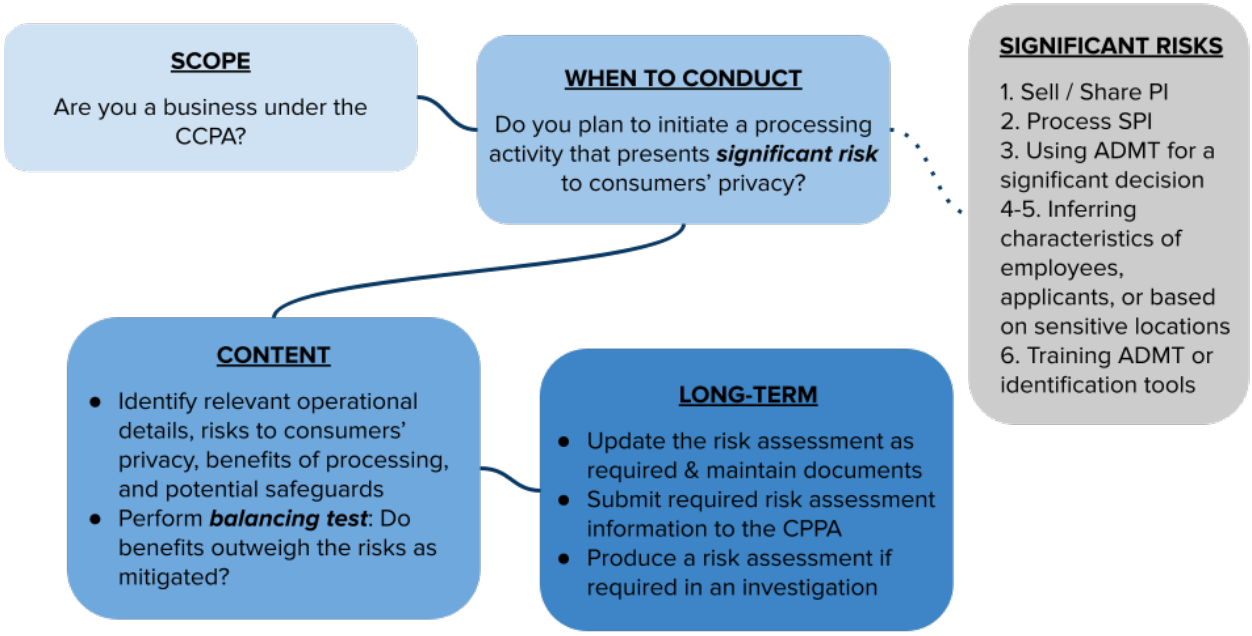
To ease compliance, the regulations allow a business that has used an ADMT more than four times in a 12-month period with respect to a consumer to provide an ***aggregate-level response***, for example, disclosing which parameters, on average, affected outputs for that consumer over the preceding year. Nothing prohibits businesses from offering additional detail beyond the minimum requirements. Aggregate responses may ease compliance but do not eliminate recordkeeping requirements. The option to provide average parameters over a 12-month period reduces the burden of individualized reporting but, to provide even an aggregate response, businesses must still maintain logs of when and how ADMT was used for each consumer.

D. Timeline

The ADMT requirements have one-year of lead time: A business that uses automated decision-making technology (ADMT) for a significant decision prior to **January 1, 2027**, must comply with the ADMT requirements by that date. Any ADMT use after the start of 2027 must comply with the relevant rules prior to being implemented. This timeline offers existing businesses a limited grace period, but places immediate obligations on future deployments.

II. Risk Assessments

Privacy professionals are accustomed to conducting risk assessments, whether required by law, self-regulatory frameworks, or internal risk management practices.[14] By adding risk assessment requirements, the updated regulations align the CCPA with the majority of other U.S. state comprehensive privacy laws, which require controllers to conduct data protection assessments for processing activities that present a heightened risk of harm to consumers.[15] The goal of a risk assessment, as identified in the regulations, is "restricting or prohibiting the processing of personal information if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public." (§ 7154.) At a high-level, the risk assessment regulations require businesses to: (1) identify processing activities that present a significant risk to consumers' privacy; (2) document relevant operational details, risks posed to consumers, benefits of the processing activity, and potential safeguards or mitigations; (3) weigh the benefits of the activity against its risks, as mitigated; and (4) maintain risk assessments and update them as necessary.



[14] Depending on the legal context, sometimes called a "privacy impact assessment," "data protection impact assessment," or a "data protection assessment."

[15] Jordan Francis, *Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends* 14–15 (Nov. 2024), https://papers.ssrn.com/id=5309115.

This section of the issue brief covers:

- **The scope of risk assessment requirements;**
- **The requirements for conducting the risk assessment,** including the content, timing, and stakeholder participation; and
- **The reporting of risk assessment information** to the CPPA and ongoing maintenance of risk assessments.

There are some key terms used throughout this section which are confusingly similar: ***"risk assessment"*** refers to the entire risk assessment process conducted pursuant to Article 10 of the regulations; ***"risk assessment report"*** refers to the documentation of a risk assessment that must be disclosed to the CPPA or AG upon request, and includes much of the content of the risk assessment; and ***"risk assessment information"*** refers to the non-content information that must be submitted to the CPPA as a matter of course (e.g., who approved the assessment and when).

How do California's Risk Assessments Compare Globally? Adding a risk assessment requirement brings the CCPA further into alignment with the majority of U.S. state comprehensive privacy laws and other notable data protection regulations from around the world, such as the General Data Protection Regulation (GDPR), which typically require impact assessments for high-risk data processing activities. The Appendix to this report includes a comparison chart that shows similarities and differences between risk assessments under the CCPA, data protection assessments under the Colorado Privacy Act (CPA), and data protection impact assessment requirements under the GDPR. Overall, there is significant overlap between what is required under the CCPA and CPA. The assessment requirements under both of those laws are more detailed, prescriptive, and rigid than the GDPR's DPIA requirements.

A. Scope

A business subject to the CCPA must conduct a risk assessment before processing consumers' personal information in a manner that presents ***significant risk to consumers' privacy***. (§ 7150, subsec. (b).) The regulations provide a fixed list of six processing activities that present significant risk to consumers' privacy, which could be updated in future rulemakings:

1. ***Selling / sharing*** personal information.
2. Processing ***sensitive personal information*** (except for processing employees' or independent contractors' sensitive personal information solely and specifically for certain listed purposes, such as administering compensation and employee benefits or providing legally required accommodations).
3. Using ***ADMT*** for a significant decision concerning a consumer.
4. Using automated processing to ***infer or extrapolate*** a consumer's

a. intelligence,
b. ability,
c. aptitude,
d. performance at work,
e. economic situation,
f. health, including mental health,
g. personal preferences,
h. interests,
i. reliability,
j. predispositions,
k. behavior,
l. location, or
m. movements

based upon ***systematic observation*** of that consumer while acting in their capacity as an educational program applicant, job applicant, student, employee, or independent contractor for the business.

5. Using automated processing to ***infer or extrapolate*** a consumer's

a. intelligence,
b. ability,
c. aptitude,
d. performance at work,
e. economic situation,
f. health, including mental health,
g. personal preferences,
h. interests,
i. reliability,
j. predispositions,
k. behavior, or
l. movements

based upon the consumer's presence in a ***sensitive location***.

6. Processing consumers' personal information which the business ***intends to use*** (is using, plans to use, permits others to use, plans to permit others to use, is advertising or marketing the use of, or plans to advertise or market the use of) ***to***

a. ***train an ADMT*** for a significant decision concerning a consumer, or
b. ***train*** a facial-recognition, emotion-recognition, or other ***technology that verifies a consumer's identity, or conducts physical or biological identification or profiling*** of a consumer.

Requiring businesses to conduct a risk assessment for ***"training"*** certain AI systems using personal information is a novel requirement amongst state comprehensive privacy laws. "Training" means the process through which a technology discovers underlying patterns, learns a series of actions, or is taught to generate a desired output. The regulations provide examples of what constitutes training, such as adjusting the parameters of an ADMT or improving the algorithm that determines how a machine-learning model learns. This definition captures any iterative process that improves or shifts an algorithm's performance, not just initial model development. Compliance obligations therefore extend beyond building new ADMTs to include any retraining or fine-tuning actions, which expands the scope of risk assessment requirements.

The regulations provide four illustrative examples of when to conduct a risk assessment:

Example 1. "Business A is hiring a new employee. Business A plans to videotape job interviews, then use emotion-recognition technology without human involvement to decide who to hire. Business A must conduct a risk assessment because it plans to use ADMT for a significant decision concerning a consumer."

Example 2. "Business B provides a mobile dating application. Business B plans to disclose consumers' precise geolocation and the ethnicity and medical information the consumers provided in their dating profiles to Business B's analytics service provider. Business B must conduct a risk assessment because it plans to process sensitive personal information of consumers."

Example 3. "Business C provides a personal-budgeting application into which consumers enter their financial information, including income. Business C plans to display advertisements to these consumers on different websites for payday loans that are based on evaluations of these consumers' personal preferences, interests, and reliability from their financial information. Business C must conduct a risk assessment because it plans to share personal information."

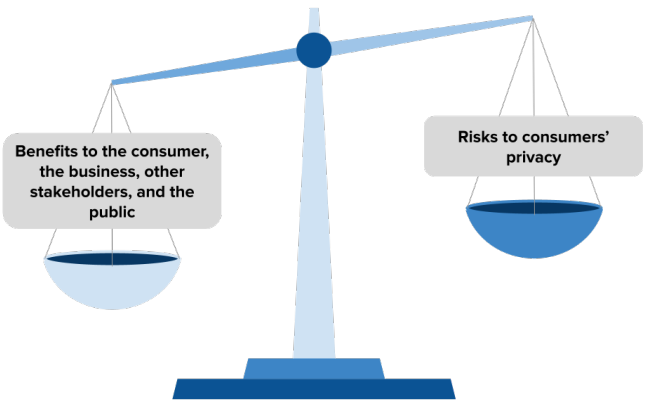
Example 4. "Business D is a technology provider. Business D plans to extract faceprints from consumers' photographs to train Business D's facial-recognition technology. Business D must conduct a risk assessment because it plans to process consumers' personal information to train a facial-recognition technology." (§ 7150, subsec. (c).)

B. Conducting the Assessment

The regulations include detailed requirements as to what a risk assessment must include and who must be involved in conducting the assessment. Although these requirements are generally aligned with requirements for conducting data protection assessments under the Colorado Privacy Act regulations[16]—the most comparable requirements in U.S. state privacy law—they are far more prescriptive than other jurisdictions, including the majority of U.S. state privacy laws.

The overarching premise of the risk assessment is a balancing test:

Do the risks to consumers' privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing?



[16] 4 Colo. Code Regs. § 904-3, Parts 8 & 9.

Conducting the balancing test first requires a detailed assessment of the processing activity's operational elements, the potential risks to consumers' privacy, the benefits posed by the activity, and potential safeguards to mitigate the risks.

1. Content

There are nine considerations or steps that go into conducting the risk assessment itself. In brief, a business must identify and document: (1) its purpose for processing consumers' personal information; (2) the categories of personal information to be processed; (3) specified operational elements of the processing; (4) the benefits of the processing activity; (5) negative impacts to consumers' privacy; (6) safeguards it plans to implement; (7) whether it will initiate the activity; (8) who (apart from legal counsel) provided information for the risk assessment; and (9) certain details about the assessment itself (e.g., date of approval, reviewers, etc).

Some of the information is required to be documented in a "risk assessment report," which can be requested by the CPPA or AG (information that must be included in a report is noted by "identify and document" rather than "identify" below). Information that does not need to be documented in the risk assessment report includes the negative impacts to consumers' privacy identified as well as the benefits to consumers, the business, other stakeholders, and the public. The specific requirements are highly prescriptive. Under § 7152, a business must identify and document the following in a ***risk assessment report***:

- The business's ***purpose*** for processing consumers' personal information, which must be identified and described with sufficient specificity. The regulations caution against using "generic terms, such as 'to improve our services' or for 'security purposes'" without additional detail (e.g., decreasing wait times to process privacy rights requests).
- The ***categories*** of personal information to be processed, including categories of sensitive personal information.

  ⚠️ This seemingly straightforward requirement is complicated by a hidden data minimization assessment lurking in this provision. Per the regulations, this "must include [identifying and documenting] the ***minimum personal information that is necessary*** to achieve the purpose of processing consumers' personal information."

- ***Operational elements*** of the processing, which include—
  - The business's planned method for processing (i.e., collecting, using, disclosing, retaining) personal information;
  - The sources of the personal information;
  - The business's method of interacting (e.g., application) with the consumers whose personal information will be processed and the purpose of the interaction;
  - The approximate number of consumers whose personal information the business plans to process;

  - What disclosures the business has or will make to the consumer about the processing activity;
  - How the above disclosures were or will be made;
  - Names or categories of service providers, contractors, and third parties to whom the consumers' personal information will be disclosed or made available for processing;
  - The purpose(s) for which the business discloses or makes available personal information to the above service providers, contractors, and third parties; and
  - If the business is using ADMT for a significant decision concerning a consumer, the business must also identify (i) the "logic of the ADMT, including any assumptions or limitations of the logic," and (ii) the "output of the ADMT, and how the business will use the output to make a significant decision."
- ***Safeguards*** that the business plans to implement, including those designed to address the negative impacts identified. The regulations provide some example safeguards, such as encryption, the use of privacy-enhancing technologies (PETs), consulting external parties to stay knowledgeable about emergent risks, and implementing procedures to ensure that ADMT works as intended and does not unlawfully discriminate. None of these are mandated.
- Whether the business will ***initiate*** the processing activity. This is contingent upon the outcome of the balancing test.
- The ***individuals***, other than legal counsel, who provided information for the risk assessment.
- The ***date*** the assessment was reviewed and approved, as well as the names and positions of the ***reviewers*** (except for legal counsel) who approved the assessment. This provision specifies that the review and approval must come from an individual who "has the authority to participate in deciding whether the business will initiate the processing that is the subject of the risk assessment."

Additionally, there are certain things that a business must ***identify*** as part of conducting a risk assessment but which are not required to be documented in the risk assessment report. These include:

- The ***benefits*** of the processing activity that flow to the business, the consumer, other stakeholders, and the public. Like with the business's processing purposes identified in the assessment, these must be identified with specificity, not with "generic terms, such as 'improving our service.'"
- The ***negative impacts*** to consumers' privacy associated with the processing, including the "sources and causes" of those impacts. The regulations provide an illustrative list of eight types of negative impacts—data breach, discrimination, impairing consumers' control over their personal information, coercing or compelling consumers into allowing

the processing of their personal information, economic harms, physical harms, reputational harms, and psychological harms.

The distinction between information that merely needs to be identified and information that needs to be identified and documented in a risk assessment report is critical, as risk assessment reports must be produced to the CPPA or AG upon request (see below).

Rigid Requirements. The list of operational elements that a business must identify is fixed. This contrasts with the approach taken in the Colorado Privacy Act regulations, which give controllers greater flexibility to decide which operational elements are relevant and at what level of detail: "[A] data protection assessment must include the following information: . . . The nature and operational elements of the Processing activity. In determining the level of detail and specificity to provide pursuant to this section, the Controller shall consider the type, amount, and sensitivity of Personal Data Processed, the impacts that operational elements will have on the level of risk presented by the Processing activity, and any relevant unique relationships." (4 Colo. Code Regs. § 904-3, Rule 8.04(a)(4).)

2. Stakeholder Involvement

The CCPA regulations dictate not only what must be in a risk assessment but also *who* must be involved. Businesses should carefully evaluate all internal and external actors who will be involved in the processing activities subject to assessment. Although the responsibility to conduct a risk assessment ultimately falls on businesses, many internal and external participants may play a role:

- **Required: *Service providers*** and ***contractors*** must, with respect to personal information that they collected pursuant to their written contract with the business, cooperate in conducting the business's risk assessment. (§ 7050, subsec. (h).) This includes "making available to the business all facts necessary to conduct the risk assessment that are in the service provider's or contractor's possession, custody, or control, and not misrepresenting any fact necessary to conduct the risk assessment." (*Id.*) This obligation must be included in the CCPA-mandated contract for service providers and contractors. (§ 7051, subsec. (a).)
- **Required:** If an ***employee's*** job duties include "participating in the processing of personal information that would be subject to a risk assessment," then the business must include that employee in its risk assessment process. (§ 7151, subsec. (a).) The regulations do not provide guidance as to when an employee's role rises to "participating" in the processing activity. The example given—"an individual who ***determines the method*** by which the business plans to collect consumers' personal information for one of the processing activities"—suggests a relatively high bar, akin to decisionmaking authority over key aspects of the processing activity. (*Id.* (emphasis added).)
- **Required: *Developers of ADMT*** have additional obligations. If a business "makes ADMT [that is trained using personal data] available to another business ("recipient-business") to

make a significant decision," then the business "must provide to the recipient-business all facts available to the business that are necessary for the recipient-business to conduct its own risk assessment." (§ 7153.) The regulations do not clarify whether making ADMT "available" means merely supplying the technology later used by a business to make significant decisions (regardless of whether that is what the developer intended) or actively marketing the technology as being ADMT for use in making significant decisions. If interpreted narrowly, this provision could apply only to businesses that market their ADMT for use in making significant decisions. If interpreted broadly, it could encompass businesses such as developers of generative AI tools who offer a general-purpose tool, so long as the recipient-business is using the tool as ADMT.

- **Optional:** A business may include ***external parties***, such as experts in detecting and mitigating bias in ADMT, consumers whose personal information the business seeks to process, or stakeholders representing consumers' interests (e.g., consumer advocacy organizations). (§ 7151, subsec. (b).)

3. No Duplicative Assessments Required

The regulations provide two important relief options to ease compliance operations for businesses. First, a business is not required to conduct multiple risk assessments for "similar processing activities that present similar risks to consumers' privacy." One assessment will suffice for a single set of "comparable" activities. (§ 7156, subsec. (a).) Second, a business that has already produced a risk assessment for another purpose (e.g., complying with another jurisdiction's privacy law) can use that assessment instead of producing a new one, provided that it contains (or can be supplemented with) all the information necessary under the regulations. (§ 7156, subsec. (b).) These exceptions for duplicative assessments are common aspects of data protection assessment requirements under U.S. state privacy laws and encourage interoperability between legal frameworks.

C. Timing and Submission Details

The lifecycle of a risk assessment includes conducting an assessment, maintaining and updating assessments, and disclosing assessments:

- **Initial Requirements.** Businesses must conduct risk assessments ***before*** initiating processing that presents significant risk to consumers' privacy. (§§ 7150 & 7155.)
- **Existing Activities.** For processing activities that satisfy one of the triggers for conducting a risk assessment but predate the updated regulations' effective date, the business must conduct a risk assessment by December 31, 2027. (§ 7155, subsec. (b).)
- **Regular Updates.** Businesses must review assessments at least once every three years and update "as necessary" to ensure accuracy and compliance with the regulations. (§ 7155, subsec. (a).)

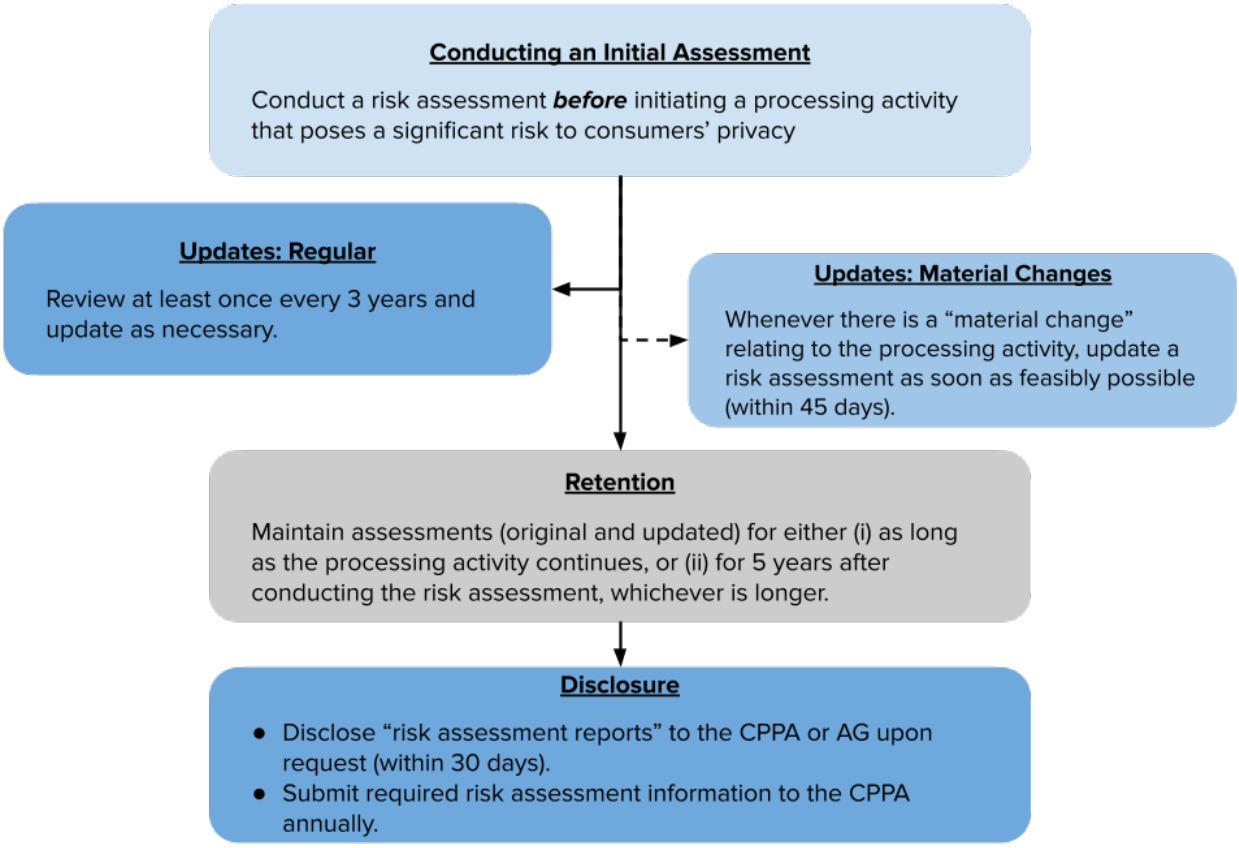
- **Updates for Material Changes.** Whenever there is a "material change" (i.e., a change relating to the processing activity that either creates new negative impacts or increases the magnitude or likelihood of previously identified negative impacts or diminishes the effectiveness of the safeguards identified in the assessment) relating to the processing activity, the business must update the risk assessment "as soon as feasibly possible, but no later than 45 calendar days from the date of the material change." (§ 7155, subsec. (a).)
- **Retention Requirements.** Businesses must maintain risk assessments (original and updated versions) for either as long as the processing activity continues, or for 5 years after conducting the assessment, whichever is longer. (§ 7155, subsec. (c).)
- **Regular Disclosures of "Risk Assessment Information."** As a matter of course, businesses must submit certain "risk assessment information" to the CPPA after conducting a risk assessment. For risk assessments conducted in 2026–27, the required information must be submitted by April 1, 2028. Starting in 2028, businesses must submit required information to the CPPA by April 1 of the following year. Information that must be submitted to the CPPA annually includes:
    - (1) Contact information;
    - (2) The time period covered by the submission;
    - (3) The number of risk assessments, both in total and per category of processing activity that triggers a risk assessment, conducted (or updated) by the business during that time period;
    - (4) Whether the risk assessments covered by the submission involved the processing of each category of personal information and sensitive information identified in the CCPA;
    - (5) Attestation that the information submitted is "true and correct"; and
    - (6) The name and title of the person submitting the risk assessment information, as well as the date of the certification.

  The risk assessment information must be submitted by a member of the business's executive management team who is ***directly responsible*** for the business's risk-assessment compliance, has knowledge of the risk assessment sufficient to provide accurate information, and has the authority to submit the risk assessment information to the CPPA. Risk assessment information will be submitted to the CPPA via the Agency's website, https://cppa.ca.gov.

Risk Assessment Information ≠ Abridged Risk Assessments: Prior drafts of the updated regulations would have required businesses to regularly submit "abridged" versions of completed risk assessments. These abridged risk assessments would have included substantive information such as why a business needed to initiate a processing activity that required a risk assessment and the protections put in place to mitigate risks to consumers' privacy. The "risk assessment information" that businesses are required to submit to the CPPA under the final regulations is substantially different.

Rather than including content of risk assessments, businesses must submit information more akin to metrics or metadata about the risk assessments they have conducted.

- **Disclosures of "Risk Assessment Reports" Pursuant to Investigations.** Businesses may be required to submit risk assessment reports at any time if requested by the Attorney general or the CPPA. The deadline to comply is 30 calendar days from the time of the request. A "risk assessment report" is the document that businesses are required to produce in conducting a risk assessment and includes the information identified in § 7152, subsecs. (a)(1)-(3), (6)-(9). (§ 7001, subsec. (zz).)



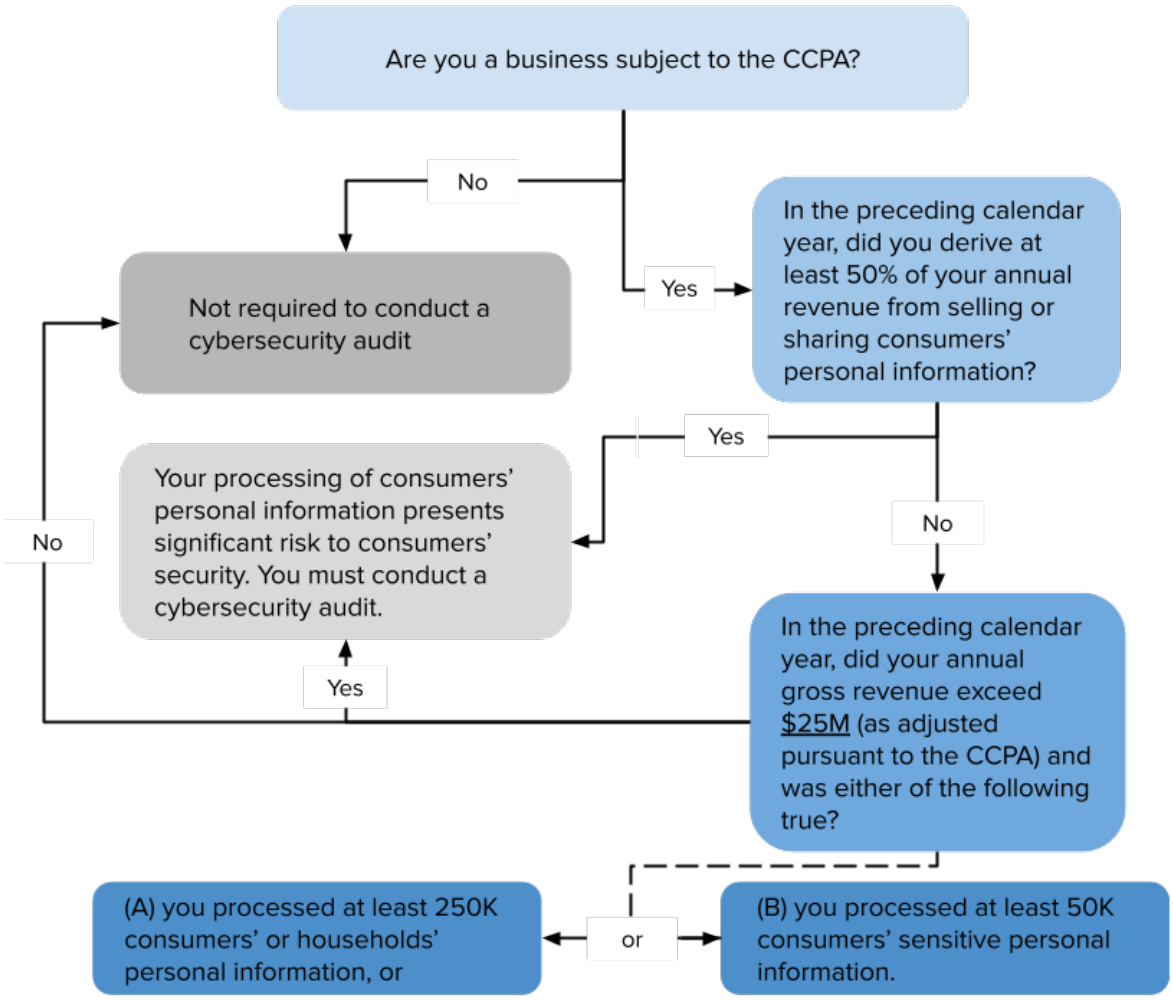
III. Cybersecurity Audits

With these new regulations, California becomes the first state to require businesses to perform cybersecurity audits under a comprehensive consumer privacy law. This section of the issue brief covers:

- **The scope of cybersecurity audit requirements;**
- **The requirements for conducting a cybersecurity audit,** including the content, timing, and stakeholder participation; and
- **The annual attestation** to the CPPA that an audit has been conducted.

A. Scope

A business must conduct an annual cybersecurity audit if its processing of consumers' personal information presents significant risk to consumers' security, which occurs under the following conditions:



Audits are meant to assess two key aspects of the business's cybersecurity program: (1) whether the program protects consumers' personal information from unauthorized access, destruction, use, modification, or disclosure; and (2) whether the program protects against unauthorized activity resulting in the loss of availability of personal information. (§ 7123, subsec. (a).)

Building out Implicit Security Requirements: Like the majority of state comprehensive privacy laws, the CCPA requires businesses that collect consumers' personal information to "implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure." (Cal. Civ. Code § 1798.100, subd. (e).) While the law does not provide required components of "reasonably security procedures and practices," the regulations implicitly provide such requirements by requiring businesses to conduct audits that consider eighteen specific components of a security program (e.g., preventing the connection of unauthorized hardware and devices to the business's information system).

B. Conducting the Audit

Like with risk assessments, there is a distinction between the ***cybersecurity audit*** that must be conducted and a ***cybersecurity audit report*** which will document certain information about the business's information system and the cybersecurity audit that was conducted.

1. Content: Audit and Audit Report

There are three areas that must be assessed in conducting a cybersecurity audit:

(1) Whether the business's establishment, implementation, and maintenance of its cybersecurity program is appropriate to the business's size, complexity, and the nature of the business's processing activities;

(2) Certain components of the business's cybersecurity program deemed applicable by the auditor to the business's information system, such as authentication, encryption of personal information, account management and access controls, and more;[17] and

(3) How the business implements and enforces compliance with its cybersecurity program. (§ 7123, subsec. (b).)

After conducting the audit, the auditor must produce a cybersecurity audit report memorializing the results. The regulations include detailed requirements as to what information must be documented in the report, including information about:

- The business's information system and certain things related to the cybersecurity audit itself, including—

[17] The regulations provide eighteen such components to consider. § 7123, subsec. (c).

    - the policies, procedures and practices assessed in the audit,
    - the criteria used for the audit, and
    - specific evidence (e.g., documents, testing, interviews) that the auditor examined to make decisions;
- Components of the business's cybersecurity program identified pursuant to § 7123, subsec. (c), including—
    - the components assessed by the auditor (both those listed in the regulations and additional components identified),
    - describing how the business implements and enforces compliance with the policies and procedures of its cybersecurity program and applicable components, and
    - the effectiveness of those policies, procedures, and components;
- Gaps or weaknesses of the business's policies and procedures and applicable components, identified and described in detail, that increase the risk to consumers' security;
- Documentation of the business's plan (including the timeframe) to address and resolve gaps or weaknesses identified;
- Any corrections or amendments to any prior cybersecurity audit reports;
- The title of "*up to three* qualified individuals responsible for the business's cybersecurity program" (emphasis added);[18]
- Information about the auditor (name, affiliation, and relevant qualifications);
- A signed and dated statement from the highest-ranking auditor certifying that their review was independent, they exercised objective and impartial judgment, and that they did not rely primarily on either assertions or attestations by the business's management, as specified in the regulations' qualifications for auditors;
- Notifications sent out under California's data breach law (Cal. Civ. Code § 1798.82); and
- Notifications sent out pursuant to another jurisdiction's data breach law.

(§ 7123, subsec. (e).) The audit report includes many requirements for the auditor to justify their findings and explain their reasoning.

2. Stakeholder Involvement

The regulations include specific requirements as to the relationship between the business and the auditor, who can be an auditor, what information the business must make available to the auditor, and what information flows between the two parties. The primary consideration for who conducts the cybersecurity audit is ***independence***. Audits must be conducted by a professional

[18] The phrase "up to three" implies a maximum but not a minimum number of individuals. Given that the report "must . . . [i]nclude" such titles, businesses should list ***at least*** one such individual.

who is qualified, objective, independent, and uses "procedures and standards accepted in the profession of auditing."[19] Auditors can be ***internal*** or ***external***, so long as they can exercise "objective and impartial judgment," are free from influence by the business being audited, and does not participate in activities that may compromise their independence (e.g., business activities that are within scope of the audit, such as implementing the business's cybersecurity program). If the auditor is internal, then "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," and any performance evaluation must be conducted by such a member of the executive management team. (§ 7122, subsec. (a).)

The regulations provide specific requirements as to what information must be made available to the auditor and how that information may be used. All relevant information in the business's possession, custody, or control must be made available to the auditor upon request. The business is under a good-faith requirement to make available—and not misrepresent—all relevant facts. (§ 7122.) In conducting the audit, findings must rely "primarily upon the specific evidence . . . that the auditor deems appropriate" and may not "rely primarily on assertions or attestations by the business's management." (§ 7122, subsec. (d).) After it has been completed, the cybersecurity audit report must be provided to a member of the business's executive management team who has direct responsibility for the business's cybersecurity program. (§ 7122, subsec. (f).)

3. No Duplicative Audit Required

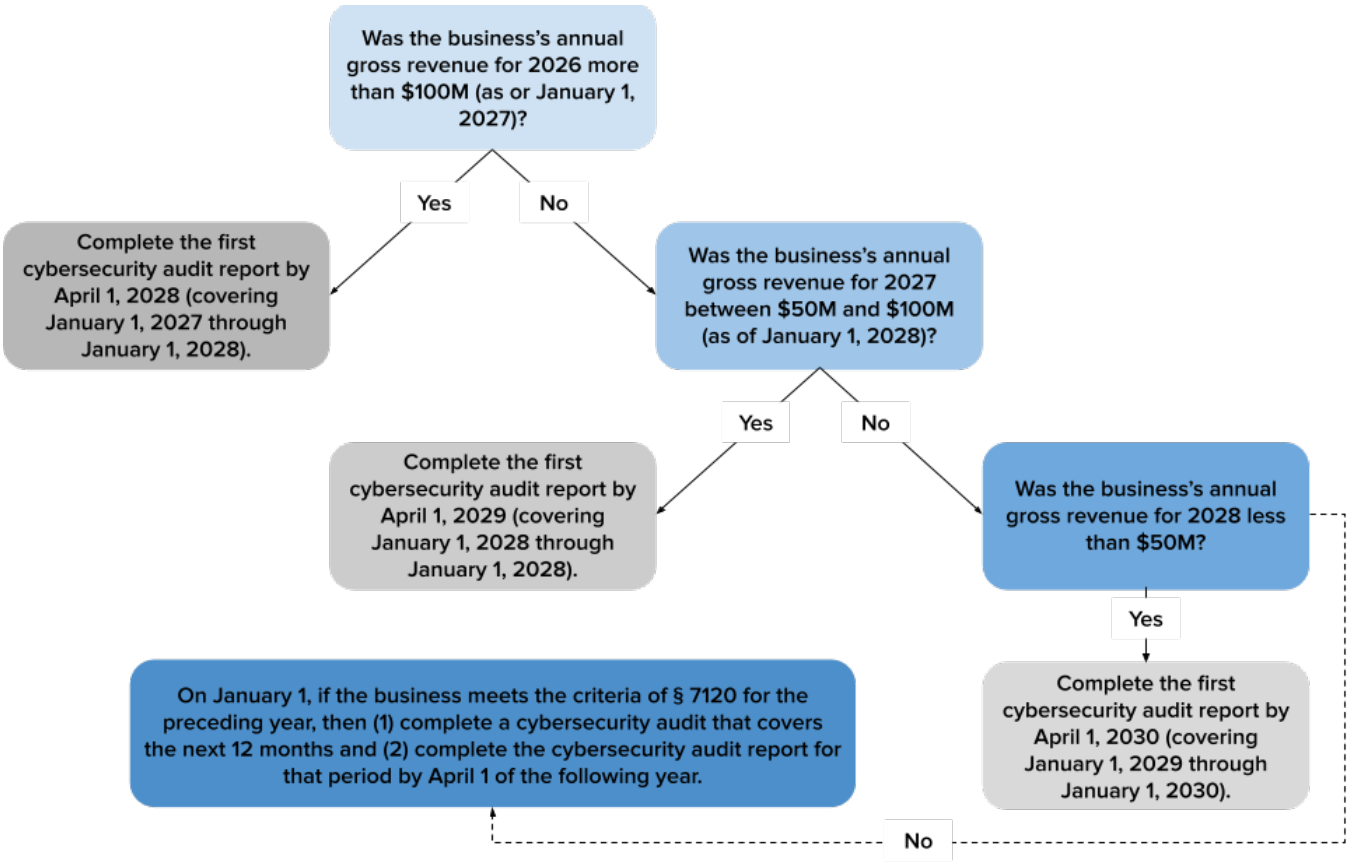
Like with risk assessments, the regulations provide flexibility for businesses that are already conducting audits under comparable regulatory or self-regulatory frameworks. If a business has already prepared a cybersecurity audit, assessment, or evaluation for another purpose and that prior process meets all of the requirements of the regulations (either on its own or when supplemented with necessary content), then the business may utilize that other work. (§ 7123, subsec. (f).)

What about ISO 27001 and SOC 2? Businesses within scope of the cybersecurity audit requirements likely already have mature information security programs and procedures. For example, organizations may already be adhering to the SOC 2 framework or have a certification of compliance for ISO/IEC 27001. Unfortunately, compliance with such industry-standard security frameworks does not directly expedite a cybersecurity audit. Although a business "may utilize a cybersecurity audit, assessment, or evaluation that it has prepared for another purpose," such as ISO/IEC 27001 compliance, that preexisting work must still meet all of the requirements of the regulations either on its own or with additional supplementation. Businesses could conduct a gap assessment to identify and address potential issues as they review current audit processes.

[19] Examples provided in the regulations include those provided or adopted by: the American Institute of Public Accountants; the Public Company Accountability Oversight Board; the Information Systems Audit and Control Association; or the International Organization for Standardization. § 7122, subsec. (a).

C. Timing and Submission Details

The lifecycle of a cybersecurity audit includes conducting an audit, maintaining audit documents, and attesting that audits have been conducted. Cybersecurity audit reports must be completed by April 1 of the year following the period covered by the audit (e.g., by April 1, 2035 for the audit covering January 1, 2034 through January 1, 2035). The time by which a business must complete its ***first*** cybersecurity audit report is staggered based on the entity's revenue, with extra lead time for smaller businesses.



For each calendar year in which a business is required to complete an audit, the business must, by the following April 1, annually submit a written certification to the CPPA that it has completed the cybersecurity audit. The certification must be completed by a qualified member of the business's executive management team, submitted at https://cppa.ca.gov, and include required contact information, the time period covered by the audit, and a signed attestation using language provided in the regulations. (§ 7124.)

After an audit report has been completed, both the business and the auditor are required to retain all documents relevant to each cybersecurity audit for at least 5 years after the audit was complete. Businesses are not affirmatively required to submit the audit report to the CPPA.[20]

IV. Additional Updates

Coverage of this rulemaking process has overwhelmingly focused on new articles concerning ADMT, risk assessments, and cybersecurity audits, but there are additional components of the rulemaking worth attention as well. In particular, the CPPA has (1) added a new article clarifying insurance companies' responsibilities under the CCPA, and (2) updated existing regulations.

A. New Regulations Clarify Insurance Companies' Responsibilities

The last new article added in this rulemaking package concerns insurance companies that are subject to the California Insurance Code and its regulations, including "insurance institutions, agents, and insurance-support organizations." Unlike many other state privacy laws, the CCPA does not broadly exempt financial institutions.[21] Rather, the law includes a data-level exemption for "personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act." (Cal. Civ. Code § 1798.145, subd. (e).) The regulations now clarify that insurance companies who qualify as a "business" under the CCPA must comply with the law with respect to any personal information not subject to the California Insurance Code and related regulations. For example, an insurance company's collection and use of employees' and job applicants' personal information would be subject to the CCPA, as would its collection of personal information from website visitors who have not applied for any insurance or financial products. (§ 7271.)

B. Updates to Existing Regulations

This rulemaking package made myriad small changes to the regulations throughout. Notable changes include—

- **Definitions:** The definitions section of the regulations is awash in changes due to the addition of many new substantive obligations with respect to ADMT, risk assessments, and cybersecurity audits. Amongst those changes, there are a few changes unrelated to those new regulations which should not be overlooked. For example, the definition of ***"sensitive personal information"*** has been added and includes "neural data," which aligns the regulations with the text of the CCPA as modified by AB 1008 in 2024. Sensitive personal

[20] The CPPA nevertheless has authority to subpoena "books, papers, records, or other items material to the performance of the agency's duties or exercise of its powers, including, but not limited to, its power to audit a business' compliance with this title." Cal. Civ. Code § 1798.199.65.
[21] *See* Jordan Francis, Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends 7-8, 22-23 (Nov. 2024), https://papers.ssrn.com/id=5309115 (discussing entity- and data-level exemptions).

information now also includes "Personal information of consumers that the business has actual knowledge [or willfully disregards] are less than 16 years of age." This is a new category of sensitive personal information that is not in the statute. Other changes fix previous oversights rather than respond to legislative updates. "Request to know" now includes requests for information about personal information ***shared***, not just sold, to third parties. (§ 7001.)

- **Increased Transparency and Notice for Opt-outs:** The updated regulations include new notice requirements for opt-out rights.
    - If a business sells or shares personal information that it collects through a ***connected device***, such as a smart television, then the business must provide notice of opt-out rights either before or at the time that the device begins collecting such information. Similarly, if a business sells or shares personal information that it collects in ***augmented or virtual reality***, then the business must provide notice of opt-out rights either (1) before or at the time that the consumer enters the augmented or virtual reality environment, or (2) before or at the time the consumer encounters the business within the augmented or virtual reality environment.[22] (§ 7013, subsec. (e).)
    - Like with the opt-out of selling or sharing personal information, businesses are also required to offer the "Notice of the Right to Limit [Processing of Sensitive Personal Information]" in the same manner in which the business collects sensitive personal information. (§ 7014, subsec. (e).) The "Notice of the Right to Limit" updates includes similar requirements to those described above concerning providing notice through ***connected devices*** and within an ***augmented or virtual reality***.
    - Businesses that receive an opt-out preference signal must now display whether they have processed the consumer's signal as a valid opt-out request. (§ 7025.)
- **Manipulative Design**: The design requirements for submitting CCPA requests and obtaining consumer consent have been amended. The "[s]ymmetry in choice" requirements now specify that opt-out requirements cannot require more steps than opting-in to the same practice, and businesses cannot make a "yes" button more prominent than a "no" button. The updated regulations also emphasize that business cannot use "misleading statements or omissions, affirmative misstatements, or deceptive language," and that "[a] consumer's silence or failure to act affirmatively does not constitute consent." The regulations similarly provide that "[a]cceptance of general or broad terms of use, or a similar document, that contains descriptions of personal information processing along with other, unrelated information" is not valid consent because "[t]his type of choice

[22] These new, heightened notice requirements for augmented or virtual reality environments were relaxed slightly from the versions introduced when rulemaking commenced. In comments to the CPPA on the draft regulations, FPF highlighted the need to "ensure flexibility in order to provide context appropriate and timely notices, as regulations should focus on quality of notices, not necessarily the format in which notices are provided." Future of Privacy Forum, Letter RE: California Consumer Privacy Act Regulations – Nov. 22 Notice of Proposed Rulemaking (Feb. 19, 2025), https://fpf.org/wp-content/uploads/2025/02/FPF-Comments-on-CPPA-Draft-Regulations-2025.02.19.pdf.

architecture prevents consent from being freely given, specific, and informed, or from signifying agreement for a narrowly defined particular purpose" (§ 7004.)

- **Consumer Rights**: The right to correction has been updated. Now, a business that complies with a consumer's request to correct inaccurate personal data must "ensure that the information remains corrected." (§ 7023, subsec. (c).)

Conclusion

These newest CCPA regulations simultaneously bring aspects of the CCPA further into alignment with existing privacy laws in other states and add novel requirements that go further than what other states have done. As the state privacy law landscape continues to mature, it is clear that the CCPA regulations will remain an ever-evolving work in progress as the CPPA continues to assess and adjust regulations in response to changing technology and policy priorities.

If you have any questions, please contact us at jfrancis@fpf.org, jgluck@fpf.org, or info@fpf.org.

Disclaimer: This issue brief is for informational purposes only and should not be used as legal advice.

FUTURE OF PRIVACY FORUM

Comparison Chart: Risk Assessment (DPIA) Requirements in California, Colorado, and the EU

	California	Colorado	EU	FPF Analysis: CA v. CO
References	**California Consumer Privacy Act (CCPA)** Cal. Civ. Code § 1798.185, subd. (a)(15) Cal. Code Reg. tit. 11, art. 10	**Colorado Privacy Act (CPA)** Colo. Rev. Stat. § 6-1-1309 Colo. Code Regs. § 904-3, Parts 8 & 9	**General Data Protection Regulation (GDPR)** Article 35 EDPB Guidelines on DPIAs	This comparison chart focuses on the updated CCPA regulations (effective Jan. 1, 2026) and comparable benchmarks under the Colorado Privacy Act. Of the various US state comprehensive privacy laws with data protection assessment requirements, Colorado was selected for comparison as having the most prescriptive requirements. **Note 1:** In 2024, Colorado enacted Senate Bill 41, adding new data protection assessment requirements for controllers that offer online services, products, or features to minors. Those minor-specific data protection assessment requirements are outside the scope of this comparison chart. **Note 2:** The GDPR's relevant DPIA requirements are provided for additional comparison, but the analysis column is focused on U.S. state privacy law.
What is the assessment called?	Risk assessment (RA)	Data protection assessment (DPA)	Data protection impact assessment (DPIA)	The term "data protection assessment" is more common in state privacy law.
When, generally, is an assessment required?	Processing consumers' personal information (PI) that presents ***significant risk to consumers' privacy***. Cal. Civ. Code § 1798.185, subd. (a)(15); § 7150.	Processing of personal data (PD) that presents a ***heightened risk of harm*** to a consumer. C.R.S. § 6-1-1309(1).	Where a type of processing is likely to result in a ***high risk to the rights and freedoms*** of natural persons. Art. 35(1).	DPAs are required where processing activities pose some heightened risk of harm. A key difference between these regulations is whether that standard is ***exhaustive or open***. Both California's and Colorado's regulations provide a list of activities that present a significant or heightened risk of harm to consumers (see next row below). California's list is ***exhaustive***—RAs are only required if a processing activity is listed in the regulations (but the Agency can add more activities in the future). Colorado, in contrast, has an ***open*** standard with an illustrative list of processing activities that meet the threshold.
Are there specific processing operations that meet the risk/harm threshold?	Yes, the following processing activities present significant risk to consumers' privacy: (1) Selling or sharing PI; (2) Processing sensitive PI (employment exceptions); (3) Using automated decisionmaking technology (ADMT) for a ***significant decision***[†] concerning a consumer; (4) Using automated processing to infer or extrapolate certain listed traits based upon systematic observation of the consumer acting in their certain capacities (e.g., job applicant, student); (5) Using automated processing to infer or extrapolate certain listed traits based upon the consumer's presence in a sensitive location; (5) Processing consumers' PI which the business intends to use (or make available to others) to (i) train ADMT for a significant decision concerning a consumer, or (ii) train technology that verifies a consumer's identity or conducts physical or biological identification or profiling. § 7150, subsec. (b). [†] A decision that results in the ***provision or denial of***, financial or lending services, housing, education enrollment or opportunity, employment or independent contracting opportunities or compensation, or healthcare services.	Yes, processing that presents a heightened risk of harm to a consumer includes: (a) Processing PD for purposes of targeted advertising or for profiling[†] if the profiling presents a reasonably foreseeable risk of: (I) unfair/deceptive treatment of, or unlawful disparate impact on, consumers, (II) financial or physical injury to consumers, (III) intrusion upon solitude / seclusion / private affairs or concerns of consumers if such would be offensive to a reasonable person, or (IV) other substantial injury to consumers; (b) Selling PD; (c) Processing sensitive data. C.R.S. § 6-1-1309(2). Rule 9.06 defines "unfair or deceptive treatment" and "unlawful disparate impact." [†] Profiling is defined consistently with other state comprehensive privacy laws as "any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."	Yes, high risk processing activities include: (a) Automated processing, including profiling,[†] leading to decisions that produce legal effects concerning the subject or similarly significantly affect them; (b) Large scale processing of special category data (Art. 9(1)) or personal data (PD) relating to criminal convictions and offences (Art. 10)); or (c) Large scale systematic monitoring of publicly accessible areas. Supervisory authorities must establish public lists of processing operations that require a DPIA and can establish lists of processing operations that do not require a DPIA. EDPB Guidelines recommend conducting a DPIA where at least two of the nine following criteria are met: • Evaluation or scoring; • Automated decisionmaking with legal or similar significant effect; • Systematic monitoring; • Sensitive data or data of a highly personal nature; • Data processed on a large scale[††]; • Matching or combining datasets; • Data concerning vulnerable data subjects; • Innovative use or applying new technological or organizational solutions; and • When processing prevents data subjects from exercising a right or using a service or a contract. Art. 35(3) & (4); EDPB Guidelines on DPIAs, at pages 9–11. [†] See Recital 71; [††] See Recital 91.	**Profiling and ADMT:** California and Colorado take different approaches with respect to profiling and ADMT. California requires RAs for ADMT used to make significant decisions, for the use of automated processing to infer certain characteristics in select circumstances, or for processing PI to train ADMT/AI capable of being used for certain purposes. This is more specific and granular than Colorado's approach, which requires DPAs for profiling that presents a reasonably foreseeable risk of certain injuries (e.g., unfair or deceptive treatment, financial injury). Drilling down into the harms to consider in a DPA, these approaches might be closer than they appear. For example, California requires businesses to consider risks like discrimination and economic harms, similar to Colorado's profiling trigger, and Colorado requires controllers to consider harms such as denial of a right or privilege such as housing or employment, which is similar to California's significant decisions trigger. **Public Monitoring:** California is unique amongst U.S. state privacy laws in explicitly requiring RAs for inferring characteristics based upon a consumer's presence in sensitive locations. Earlier drafts of the regulations would have imposed broader requirements with respect to monitoring consumers in public places. **Adolescent Privacy:** California and Colorado both require assessments for processing sensitive data. In California, the updated regulations expand the definition of sensitive personal information to cover personal information of consumers whom the business has actual knowledge are under 16. This is broader than Colorado's approach (defining the personal data from a known child under 13 as sensitive).

FUTURE OF PRIVACY FORUM

Comparison Chart: Risk Assessment (DPIA) Requirements in California, Colorado, and the EU

	California	Colorado	EU	FPF Analysis: CA v. CO
Which stakeholders should be involved?	**Required:** Any employees whose job duties include participating in the processing of PI that would be subject to a risk assessment must be included. **Optional:** A business can choose to involve external parties. (e.g., ADMT bias experts, a subset of affected individuals, and consumer advocacy groups). Consulting external parties to ensure current knowledge of emergent privacy risks and countermeasures is a safeguard that a business may consider in an assessment. §§ 7151, 7152 subsec. (a)(6)(A)(iii).	DPAs must involve ***all relevant internal actors*** and, "where appropriate," ***relevant external parties***. Rule 8.03(A).	The controller shall seek the advice of the data protection officer, where designated, when carrying out a DPIA, and, where appropriate, shall seek the views of data subjects. A controller shall consult a supervisory authority where a DPIA indicates that processing involves a high risk which cannot be mitigated by appropriate measures, or whenever member state law requires consultation before a controller carries out processing for the performance of a task in the public interest. Art. 35(2) & (9); Art. 36(1) & (5); Recital 84.	Both regimes require input from relevant internal actors. California encourages consulting with affected individuals where appropriate; Colorado does not address this. **Note:** This row omits information on whether and to what degree service providers or processors are required to assist businesses / controllers in conducting assessments.
Do assessment requirements scale?	Not explicitly.	Yes. The depth, level of detail, and scope of DPAs should take into account the scope of risk presented, size of the controller, amount and sensitivity of PD processed, PD processing activities subject to the assessment, and complexity of safeguards applied. Rule 8.02(C).	Not explicitly. The text of the GDPR does not make any differentiation based on the size of the controller, while Guidelines from the EDPB highlight that the implementation of a DPIA is scalable to the processing operations of even a "small data controller". The complexity of the processing operations and level of risk to the rights of individuals are the key factor to impact the complexity of a DPIA. EDPB Guidelines on DPIAs, at page 17.	Colorado includes an explicit statement that assessments should be tailored to the complexity and risk of the processing operations under consideration or the size of the business.
Are there exceptions?	Yes. Processing consumers' sensitive PI does not require a RA if the business is processing the employees' or independent contractors' information "solely and specifically for" certain employment related purposes (e.g., providing reasonable accommodations required by law). § 7150, subsec. (b)(2)(A).	No.	Yes. When the lawful basis for processing is Art. 6(1)(c) [compliance with a legal obligation] or (e) [performance of a task carried out in the public interest or in the exercise of official authority vested in the controller], and that obligation is based in E.U. law or the law of a Member State, and a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, then Art. 35(1)–(7) shall not apply unless a Member State deems it necessary to do so prior to processing. Additionally, Member States have the ability to publish a list of allowed processing operations. Art. 35(10); Art. 35(5).	For California and Colorado, data-level and entity-level exceptions to the underlying laws will apply to the regulations as well. The CCPA is broader than the Colorado Privacy Act in that it applies to employee and business-to-business data.

FUTURE OF PRIVACY FORUM

Comparison Chart: Risk Assessment (DPIA) Requirements in California, Colorado, and the EU

	California	Colorado	EU	FPF Analysis: CA v. CO
What are the substantive elements of an assessment? *See below for elements specific to AI, ADMT, & profiling*	(1) Identify and document the ***purpose*** for processing PI; (2) Identify and document categories of PI to be processed (and identify the ***minimum PI necessary*** to achieve the processing purpose); (3) Identify and document certain ***operational elements***† of the processing; (4) Identify ***benefits*** to the business, consumer, other stakeholders, and public from the processing; (5) Identify ***negative impacts***† to consumers' privacy; (6) Identify and document ***safeguards***† the business plans to implement; (7) Identify and document whether the business will initiate the processing subject to the RA; (8) Identify and document individuals who provided information for the RA (other than legal counsel); (9) Identify and document the date the RA was reviewed and approved and names and positions of individuals who reviewed or approved. § 7152. † Examples or requirements specified in the regulations Items (1)-(3), (6)-(9) get recorded in a "risk assessment report" that can be requested by the CPPA or AG.	DPAs must identify and describe the risks to consumers' rights associated with the processing, document measures considered and taken to address and offset risks, contemplate the processing's benefits, and demonstrate that benefits outweigh the risks as offset by safeguards. Specific elements: (1) Short summary of the processing activity; (2) Categories of PD to be processed (including whether they include sensitive data); (3) Context of the processing activities (including the controller's and consumers' relationship and consumers' reasonable expectations); (4) Nature and operational elements of the processing; (5) Core purposes of the processing activity and other benefits that may flow to the controller, consumer, other stakeholders, and the public; (6) Sources and nature of risks to consumers' rights; (7) Safeguards to be employed; (8) Description of how the benefits outweigh the risks (as mitigated by safeguards); (9) For profiling (see C.R.S. § 6-1-1309(2)(a)), the DPA must also comply with Rule 9.06 (see below); (10) For processing sensitive data, details of the process implemented to ensure that PD and sensitive data inferences are not transferred and are deleted with 24 hours of the processing activity; (11) Relevant internal actors and external parties contributing to the DPA; (12) Any internal/external audit conducted for the DPA, including details about the auditor or individuals involved; (13) Dates DPA was reviewed and approved; and names, positions, and signatures of those responsible. Rule 8.02(A); Rule 8.04.	In conducting a DPIA, a controller should take into account the nature, scope, context and purposes of the processing and the sources of risk. DPIAs shall contain at least: (a) A description of the envisaged processing operations and the purposes of the processing; (b) An assessment of the necessity and proportionality of the processing; (c) An assessment of the risks to the rights and freedoms of data subjects; and (d) Measures envisaged to address the risks and demonstrate GDPR compliance. Art. 35(7); Recital 90. Note: The assessment of the risks to the rights and freedoms of data subjects is broader than just "privacy" risks. Rather, it concerns all rights and freedoms that may be impacted by the processing operations, which may include freedom of speech, due process, non-discrimination, etc. EDPB Guidelines on DPIAs, at page 6.	***Operational Elements:*** One notable difference between California and Colorado is the level of specificity required in detailing operational elements of the processing. The Colorado regulations afford controllers some flexibility in determining the level of detail and specificity to provide and list relevant operational elements that ***may*** be included. California, in contrast, provides a lengthier list of required considerations. ***Weighing Risks and Benefits:*** Another notable difference is the framing of the ultimate balancing test. Colorado's regulations require that DPAs include a "description" of how the benefits outweigh the risks as mitigated by safeguards. Given the inherent difficulty in quantifying and comparing risks and benefits in this context, Colorado's standard could ease concerns about good faith estimates of the balance of risks and benefits being second guessed by regulators. Prior drafts of California's regulations would have expressly prohibited proceeding with a processing activity if the risks to consumers' privacy outweighed the benefits. The final regulations, however, soften that requirement by stating the the "goal" of a risk assessment is "***restricting or prohibiting*** the processing of personal information" if the risks outweigh the benefits. This aspirational framing—describing the "goal" but not an affirmative obligation not to proceed— suggests that the final regulations are less strict than prior drafts.
What harms or risks should be considered?	Negative impacts to consumers' privacy include: (A) Security harms (e.g., unauthorized access); (B) Discrimination on the basis of protected characteristics; (C) Impairing consumers' control over their PI; (D) Coercing or compelling consumers into allowing processing of their PI; (E) Economic harms; (F) Physical harms to consumers or property; (G) Reputational harms; (H) Psychological harms; § 7152, subsec. (a)(5).	Risks to the rights of consumers may include: (a) Constitutional harms; (b) Intellectual privacy harms; (c) Data security harms; (d) Discrimination harms; (e) Unfair, unconscionable, or deceptive treatment; (f) A negative outcome/decision with respect to an individual's eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-case services, or access to essential goods or services; (g) Financial injury or economic harm; (h) Physical injury, harassment, or threat to an individual or property; (i) Privacy harms, such as intrusion upon solitude/seclusion/private affairs or concerns of consumers, stigmatization, or reputational injury; (j) Psychological harm; (k) Other detrimental or negative consequences that affect an individual's private life or similar concerns where an individual has a reasonable expectation that personal data or other data will not be collected, observed, or used. Rule 8.04(A)(6).	Risk to the rights and freedoms of natural persons may result from personal data processing which could lead to physical, material or non-material damage, resulting from the following processing operations / situations: • Processing that may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of PD protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; • Where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their PD; • Where PD are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; • Where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; • Where PD of vulnerable natural persons, in particular of children, are processed; or • Where processing involves a large amount of PD and affects a large number of data subjects. Recital 75.	California and Colorado have a slight difference in approach tied to the triggers for an assessment (see above). For example, Colorado requires DPAs for uses of profiling that present a reasonably foreseeable risk of certain injuries and then considers a negative outcome with respect to an individual's eligibility for a right, privilege, or benefit to be a harm worth considering. California instead treats the use of ADMT to make a significant decision as a trigger for a DPA, then requires consideration of harms such as economic injury or discrimination.

FUTURE OF PRIVACY FORUM

Comparison Chart: Risk Assessment (DPIA) Requirements in California, Colorado, and the EU

	California	Colorado	EU	FPF Analysis: CA v. CO
What safeguards should be considered?	Safeguards a business ***may*** consider include: (i) Encryption, segmentation, access controls, change management, network monitoring and defenses, and data and integrity monitoring; (ii) Use of ***PETs*** (e.g., trusted execution environments, federated learning, homomorphic encryption, differential privacy); (iii) Consulting external parties to ensure current knowledge of emergent privacy risks and countermeasures; and (iv) Implementing policies, procedures, and training to ensure that the business's ADMT works for the intended purpose and does not unlawfully discriminate. § 7152, subsec. (a)(6)(A).	Measures considered ***shall*** include: (a) Use of de-identified data; (b) Measures taken pursuant to controller duties (e.g., data minimization, avoiding secondary use, etc.), including an overview of data security practices implemented, data security assessments completed, and measures taken to comply with consent requirements. (c) Measures taken to ensure consumers have access to rights provided in C.R.S. § 6-1-1306 (opt-out, access, correction, deletion, data portability). Rule 8.04(A)(7).	EDPB Guidelines provide examples of measures that can be appropriate safeguards, such as: • Pseudonymization; • Encryption of PD; • Data minimization; • Oversight mechanisms; etc. EDPB Guidelines on DPIAs, at 19.	California and Colorado both provide examples of safeguards to consider but neither require that those specific safeguards be implemented.
Do assessments prohibit certain processing activities?	Unclear. The stated "goal" of a risk assessment is ***restricting or prohibiting*** the processing of PI if the risks to consumers' privacy outweigh the benefits resulting from processing (to the consumer, business, other stakeholders, and public). Prior drafts explicitly stated not to initiate the activity if the risks outweigh the benefits. § 7154.	Yes. A DPA must "demonstrate[ ] that the benefits of the Processing outweigh the risks offset by safeguards in place." Rule 8.02(A).	Unclear. There is no explicit statement not to engage in processing if the risks outweigh the benefits, but there is a requirement to consult with a supervisory authority if risks cannot be mitigated. The supervisory authority may use its Art. 58 powers if it determines that the intended processing would infringe the GDPR. Art. 36; Recital 84.	Colorado stands alone in clearly and unequivocally telling controllers not to proceed with a processing activity if the risks outweigh the benefits.
What is the timing for conducting an assessment?	Before initiating any processing activity that presents a significant risk to consumers' privacy. § 7155, subsec. (a)(1).	Before initiating a processing activity that presents a heightened risk of harm to a consumer. Rule 8.05(A).	Before initiating processing that is likely to result in a high risk to the rights and freedoms of natural persons. GDPR Recital 90.	California and Colorado are aligned with one another but inconsistent with the majority of enacted US state comprehensive laws which, with the exception of New Jersey, do not explicitly require that the assessment occur *before* initiating processing. Such a requirement could raise First Amendment challenges.
When should assessments be updated?	**Material changes:** Update a RA whenever there is a material change† in the processing activity. This must be done as soon as feasibly possible but no later than 45 calendar days. **In general:** Review, and update as necessary, at least once every three years. § 7155, subsec. (a)(2)-(3). † A change is material if it creates new negative impacts, increases the magnitude or likelihood of negative impacts, or diminishes the effectiveness of safeguards.	**Material changes:** A DPA shall be updated when existing processing activities are modified in a way that materially changes the level of risk presented (example list provided in Rule). **In general:** Review and update DPA as often as appropriate throughout the processing activity's lifecycle, to: (1) monitor for harm caused by the processing and adjust safeguards; and (2) ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing. **Profiling:** DPAs for profiling in furtherance of decisions that produce legal of similarly significant effects concerning a consumer shall be reviewed and updated at least annually, with an updated evaluation for fairness and disparate impact. Rule 8.05(C) & (D).	**Change of risk:** A controller shall carry out a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk presented by processing operations. EDPB Guidelines suggests that DPIAs should be continuously reviewed and regularly reassessed. Art. 35(11); EDPB Guidelines on DPIAs, at page 14.	**Material Changes:** Both regimes require that assessments be updated when there is a sufficient change in the risk posed, which can happen due to technological, society, or organizational reasons. **Cadence:** These regimes differ as to whether assessments should be regularly reviewed and updated. California opted for a set cadence of once every 3 years to review and update DPAs. Colorado opted for the flexible standard that assessments be updated as appropriate. **ADMT / Profiling:** Another difference between regimes is whether DPAs regarding ADMT or profiling are singled out for special update requirements. California does not have ADMT- or profiling- specific update requirements, whereas Colorado requires annual review and updates for assessments concerning profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.
How long do you retain assessments?	Retain RAs (originals and updated versions) for as long as the processing continues or **five years** after the completion of the RA, whichever is later. § 7155, subsec. (c).	Retain DPAs (including prior versions which have been revised when a new processing activity is generated) for as long as the processing continues and at least three years after the activity's conclusion. Retain DPAs in an electronic, transferable form. Rule 8.05(E).	There is no explicit requirement to retain DPIAs for a certain amount of time after a processing activity concludes, but a controller is still subject to general record-keeping obligations to demonstrate GDPR compliance. See Art. 24.	California is slightly stricter than Colorado, requiring that assessments be retained for two years longer.
Are retroactive assessments required?	Yes. For any processing activities initiated prior to January 1, 2026 and that continues after that date, the business must conduct and document a risk assessment by December 31, 2027. § 7155, subsec. (c).	No, the DPA requirements apply to activities created or generated after July 1, 2023 and are not retroactive. However, a new processing activity is generated when changes to existing activities result in a material changes to the level of risk presented, in which case a DPA may be required. C.R.S. § 6-1-1309(6); Rule 8.05(D), (F).	New DPIAs are not required for processing operations initiated before the GDPR's effective date, but (1) the Article 29 Working Party Guidelines recommends carrying out DPIAs for all high risk operations prior to that date, and (2) a DPIA may have to be conducted or updated where there is a change in the processing activity or risk, as set out in Art. 35.	California's rule is stricter than Colorado's, requiring assessments for ongoing operations at the time of the effective date. Colorado, in contrast, requires assessments only for new activities. Both regimes are still subject to their respective obligation to update assessments (or conduct one in the first instance) in response to changes to processing operations or the risks of harm.
Can one assessment cover multiple processing operations?	Yes, a single RA can cover a "comparable set of processing activities" (defined as "a set of similar processing activities that present similar risks to consumers' privacy"). § 7156, subsec. (a).	Yes, a single DPA may address a "comparable set of Processing operations" (defined as "a set of similar Processing operations including similar activities that present heightened risks of similar harm to a Consumer"). C.R.S. § 6-1-1309(5); Rule 8.02(D).	Yes, a single assessment may address a set of similar processing operations that present similar high risks. Art. 35(1).	California and Colorado are consistent on this issue.

FUTURE OF PRIVACY FORUM

Comparison Chart: Risk Assessment (DPIA) Requirements in California, Colorado, and the EU

	California	Colorado	EU	FPF Analysis: CA v. CO
Can an assessment conducted for the purpose of complying with another jurisdiction's law or regulation satisfy the requirement?	Yes, a business can utilize a risk assessment prepared for another purpose provided that it meets all the requirements of this regulation. An insufficient RA can be supplemented to satisfy the regulations. § 7156, subsec. (b).	Yes, if the assessment is reasonably similar in scope and effect, or if the controller submits that assessment with a supplement that contains any additional information required by CO. Rule 8.02(B).	According to EDPB Guidelines, "The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them." In any case, a DPIA must meet the requirements in Art. 35(7) to be considered valid under the GDPR. EDPB Guidelines on DPIAs, at page 17.	California and Colorado are consistent on this issue.
When, to whom, and in what form must assessments be submitted?	**Annual:** Businesses will have to annually submit certain ***"risk assessment information"*** (RAI) to the CPPA. For RAs conducted in 2026-27, this must be done by April 1, 2028. After that, submissions must be by April 1 of the following year. The required RAI to submit includes contact information for the business, the time period covered, the number of RAs conducted during that period (total and by type of processing activity), whether the RAs conducted during that period involve the processing of each of the categories of PI and SPI in the CCPA, attestation that the risk assessment information is "true and correct," name and title of the submitter, and the date. Submissions of RA materials are made via the CPPA website. **On Request:** Businesses must make ***"risk assessment reports"*** available to CPPA or AG upon request (30 calendar days). Risk assessment reports include most (but not all) of the content of the risk assessment. § 7157.	**On Request:** Controllers must make DPAs available to AG within 30 days of request. Rule 8.06.	DPIAs are not required to be published, but EDPB Guidelines suggest publishing at least parts (e.g., summary or conclusion) to foster trust and demonstrate compliance. Supervisory authorities may review DPIAs as part of their Art. 58 powers. Recital 89; EDPB Guidelines on DPIAs, at page 18.	Both regimes require a business / controller to submit an assessment to the Attorney General upon request, and both have a 30 day deadline for compliance with such requests. California differs in that business will be required to annually submit certain "risk assessment information." Absent from California's draft regulations are protections against public records requests and waiver of attorney-client privilege or work-product protections. (*See* Colo. Rev. Stat. § 6-1-1309(4).) Failing to provide protections like those in the Colorado Privacy Act could result in businesses producing assessments that are less candid.
Are there additional requirements regarding AI, ADMT, or profiling?	**RA Triggers:** There are three categories of processing activities involving ADMT or automated processing that require RAs: • Using of ADMT for a significant decision; • Using automated processing to infer or extrapolate certain characteristics about a consumer either while they are acting in certain capacities or based upon their presence in a sensitive location; and • Processing PI to train an ADMT or certain technology used for identification or physical or biological profiling. **Opt-Out:** Although not within scope of this chart, the regulations also include rights of notice, access, and opt-out with respect to certain uses of ADMT and AI. **Developer Disclosures:** A business that makes ADMT available to another business for making a significant decision must provide all facts necessary for the recipient to conduct its own RA. § 7153.	**DPA Triggers:** Profiling requires a DPA if it presents a reasonably foreseeable risk of: 1. unfair or deceptive treatment of, or unlawful disparate impact on, consumers; 2. financial or physical injury to consumers; 3. physical or other intrusion upon the solitude/seclusion or private affairs/concerns of consumers if it would be offensive to a reasonable person; 4. or other substantial injury to consumers. Rule 9.06(A). For profiling-specific DPA requirements, see below. **Opt-out:** Although not within scope of this chart, the regulations also include opt-out rights with respect to profiling in furtherance of decisions that produce legal or other similarly significant effects concerning a consumer. This does not align 1:1 with the types of profiling that require a DPA. **Standalone AI Law:** In 2024, Colorado enacted a law regulating development and deployment of high-risk AI systems that make or are a substantial factor in making consequential decisions affecting individuals. That law includes impact assessment requirements. That law is outside the scope of this comparison chart. For more information, see FPF's Policy Brief on the Colorado AI Act.	ADMT under the GDPR is generally beyond the scope of this chart. For a detailed overview of the subject, see FPF's prior report on Automated Decision-Making Under the GDPR. **DPIA Triggers:** Evaluations and decisions that are based on automated decisionmaking with legal or similar effects, including profiling, and forms of evaluation or scoring are singled-out as examples of processing activities likely to result in high risks to fundamental rights and freedoms of individuals. **Transparency Requirements:** Use of ADMT triggers certain transparency requirements, such as informing data subjects about the existence of and logic involved in ADMT used and explaining the significance and envisaged consequences to the data subject, and opt-out/contestability rights. Art. 35(3); Recital 71; EDPB Guidelines on DPIAs, at pages 8-9; EDPB Guidelines on Profiling, at page 27. **EU AI Act:** Although outside the scope of this comparison chart, it is important to note that the EU AI Act also requires that certain deployers must, before deploying a high-risk AI system identified in EU AI Act Art. 6(2), perform a fundamental rights impact assessment (FRIA). EU AI Act, Art. 27.	California and Colorado use different terms. California refers to ADMT, which includes profiling, whereas Colorado refers to profiling. California also has provisions concerning "automated processing," which is undefined but presumably distinct from ADMT or profiling. Both regimes have specific opt-out rights and transparency requirements for use of ADMT or profiling. California and Colorado differ as to when use of ADMT or profiling triggers an assessment. See that analysis above under "Are there specific processing operations that meet the risk/harm threshold?"

FUTURE OF PRIVACY FORUM

Comparison Chart: Risk Assessment (DPIA) Requirements in California, Colorado, and the EU

	California	Colorado	EU	FPF Analysis: CA v. CO
What additional elements must an assessment include for AI , ADMT, or profiling?	Businesses must conduct RAs for using ADMT to make a significant decision concerning a consumer and for training certain AI systems. If the business is using ADMT to make a significant decision, then two operational elements that must be identified and documented in a risk assessment report are the "logic of the ADMT, including any assumptions or limitations of the logic" and the "output of the ADMT, and how the business will use the output to make a significant decision." One of the suggested safeguards that a business may consider to mitigate privacy risks to consumers is "[i]mplementing policies, procedures, and training to ensure that the business's ADMt works for the business's purpose and does not unlawfully discriminate based upon protected characteristics." § 7152.	DPAs for profiling must include the elements required under Rule 8.04 as well as the following profiling-specific elements: (1) Types of PD used in the profiling; (2) The decision to be made using profiling; (3) Benefits of automated processing over manual processing; (4) Plain language explanation of why the profiling directly and reasonably relates to the controller's goods and services; (5) Explanation of the training data and logic used to create the profiling system; (6) Information about purchased third-party software used; (7) Plain language description of outputs; (8) Plain language description of how the outputs will be used, including use for consequential decisions; (9) Information about the degree of human involvement; (10) How the profiling system is evaluated for fairness and disparate impact (and the results of evaluations); (11) Safeguards used to reduce the risks of harms identified; (12) Safeguards for data sets produced by/derived from profiling. Rule 9.06.	Controllers should look to other GDPR provisions concerning ADMT and transparency (e.g., Arts. 13, 14, & 22) when evaluating risks and safeguards in a DPIA. EDPB Guidelines on DPIAs, at page 27. **EU AI Act:** As mentioned above, the EU AI Act includes an FRIA requirement for certain deployers of high-risk AI systems. EU AI Act, Art. 27.	Colorado has more detailed requirements, including an explanation of fairness and disparate impact testing in addition to other required explanations.

1350 Eye Street NW Suite 350
Washington, DC 20005

info@fpf.org

FPF.org