FSOR APPENDIX B – SUMMARIES AND RESPONSES TO 15 DAY COMMENTS

ARTICLE 1. GENERAL PROVISIONS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7001	385, 386	Comment states that the key definitions are overly broad and regulate tools beyond the Agency's intended scope. Comment states that the key definitions do not have a meaningful connection to privacy and create unnecessary compliance risks for businesses without reducing risks for consumers.	The Agency disagrees with this comment. The definitions are within the Agency's authority and are tailored to further the intent and purposes of the CCPA to protect consumer privacy. They provide clarity and guidance about the types of tools that are in scope of the regulations. They are also adaptable to a variety of contexts and work with the requirements in the regulations to provide both privacy protections for consumers and flexibility for businesses.
Previous 7001(c)	104, 373	Comment supports deleting the definition of artificial intelligence, which previously over-expanded the scope. The regulations remove references to AI and instead focus on ADMT. This change decreases the potential for the ADMT rules to apply to broader AI systems in ways that are confusing and impractical.	The Agency notes commenter's support. The Agency disagrees with this comment to the extent it suggests that the proposed regulations were confusing, impractical, or over-expanded the scope. Nevertheless, exercising its discretion, the Agency removed references to artificial intelligence to further simplify implementation at this time. Since the CCPA and these regulations protect consumers' privacy, regardless of the particular technology at issue, they can still apply to personal information processed by artificial intelligence whether stated expressly or not.
Previous 7001(c)	581	Comment raises concerns that the removal of AI from the regulations could create a loophole, allowing companies to claim that their algorithms and automated decisions are actually AI and therefore exempt. Comment suggests that the Agency should re-incorporate AI into in § 7001(e).	The Agency disagrees with this comment. The regulations apply to the use of ADMT, which includes any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking. The ADMT requirements apply when a business uses ADMT to make a significant decision, including when the ADMT leverages AI.
7001(e)	53, 80, 100, 102, 196, 214,	Comment expresses concern that the revised definition of ADMT remains overly broad and not limited to significant decisions. Comment argues that even with changes to the	The Agency disagrees with this comment. The definitions are within the Agency's authority and are tailored to further the intent and purposes of the CCPA to protect consumer privacy.

	284, 323, 439	definition of "automated," the rules still appear to apply to common, decades-old, business tools. Comment warns this could include nearly all automated processes, even routine ones, like hiring platforms, inventory systems, and basic software systems that are used for everyday functions like analyzing employee performance, tracking safety metrics, or determining eligibility for routine bonuses, which is not what voters intended when they approved Proposition 24. Comment suggests further amendments to limit the scope of the definition would help to focus the rules' impact to processing that presents actual risks to consumers. Without amendments to refine and clarify the definition's scope, the regulations could lead to unintended consequences that extend beyond their intended purpose. Comment urges the Agency to adopt a more targeted, risk-based approach. Comment recommends narrowing the scope of ADMT to only include systems that make final decisions using machine learning with legal or significant effects. Comment urges the Agency to provide clear thresholds and carve-outs for low-risk or operational ADMT uses that do not materially impact consumer rights or access, and clarify how "human involvement" is evaluated in practice, especially for businesses with limited staffing resources. Comment also recommends discussions to ensure alignment between proposed state AI legislation and this rulemaking to avoid conflicting definitions of "consequential" and "significant" decisions.	The definition of ADMT is not overly broad but rather addresses a higher-risk use of ADMT, which is one without human involvement. The Agency has determined that a business's use of ADMT to make significant decisions presents significant risk to consumers' privacy and requires a risk assessment. Further, it also significantly impacts consumers, and the regulations accordingly require Pre-use Notices, opt-out and access rights for that use of ADMT. Only ADMT that are used to make significant decisions about consumers without human involvement are subject to these requirements; it would therefore be redundant to add the term "significant decision" into the definition of ADMT. The regulations are consistent with other privacy frameworks within the state and in other jurisdictions. The definition already provides criteria to clarify the threshold of human involvement. The Agency believes that no further clarification is needed at this time. The Agency looks forward to continuing to work with stakeholders, including the Legislature and Governor Newsom, on future policy development.
7001(e)	55, 336, 388, 451, 489, 542	Comment supports limiting ADMT obligations to not involve human review and that are used to make significant decisions. However, the statement in § 7001(e)(2) that ADMT "includes profiling" could cause some confusion and potentially undermine these goals, particularly given the broad definition of "profiling." Comment suggests that this creates confusion because the "profiling" definition goes beyond profiling for "significant decisions." Comment	The Agency disagrees with this comment. The CCPA states that ADMT includes profiling. (*See* Civ. Code § 1798.185(a)(15).) The CCPA also defines "profiling" and directs the Agency to further define it. (*See* Civ. Code §§ 1798.140(z), 1798.185(a)(15).) The regulations implement the CCPA and ensure consistency with how the CCPA addresses the creation of profiles in its definition of "personal information." (*See* Civ. Code § 1798.140(v)(1)(K).) The regulations' definitions do not impose regulatory

		recommends clarifying that "profiling" in the ADMT context only extends to "significant decisions." Otherwise, businesses may face uncertainty over whether, for example, even banal processing activities, such as personalizing the content shown to consumers using solely data collected in a first-party context, require adherence to the ADMT-specific obligations set forth in the regulations. Comment recommends revising § 7001(e)(2) as follows: "ADMT includes profiling when used to make a significant decision." Comment objects to the revised definition of ADMT and expanded definition of "profiling," arguing that the regulations would broaden the statutory definition of "profiling" in a manner which would result in further expanding the definition of ADMT. The expansion of the "profiling" definition amplifies the complexity and potential impact of the ADMT definition. The current draft of § 7001(e)(2) could be misinterpreted to suggest that all profiling should be deemed ADMT whether or not it replaces human decisionmaking. Comment proposes revision as follows: (1) § 7001(e)(2): "ADMT includes profiling that replaces or substantially replaces human decisionmaking." Comment states that the key definitions, such as the definition for "profiling" in § 7001(e)(2), create unnecessary compliance risks for businesses without reducing risks for consumers. The definition of ADMT still considers profiling to count as ADMT which could capture common business technologies such as technology designed to track and analyze worker behavior even without any decisionmaking based on the profiling and does not present any privacy risks.	requirements upon businesses, nor do they create complexity. Rather, they provide clarity regarding the types of technology and profiling that are subject to the ADMT requirements. The regulations are clear that profiling that replaces or significantly replaces human decisionmaking for a significant decision is subject to the requirements of Article 11. The Agency does not believe that further clarification is necessary at this time. Nevertheless, the Agency modified § 7001(e)(2) to explicitly state that profiling "that replaces human decisionmaking or substantially replaces human decisionmaking" is in scope of the definition of ADMT.
7001(e)	73	Comment argues that the current language continues to exceed statutory limits by regulating tools that merely "substantially replace" human decisionmaking. Comment argues that it should apply only to fully automated systems that independently process personal data.	The Agency disagrees with this comment. The CCPA's delegation to the Agency regarding ADMT is not limited to "solely" automated decisionmaking. Rather, the CCPA directs the Agency to issue regulations governing access and opt-out rights "with respect to a business' use of automated decisionmaking

			technology, including profiling." (*See* Civ. Code § 1798.185(a)(15).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) The ADMT regulations are within the Agency's authority, further the intent and purpose of the CCPA, and are necessary to address the use of ADMT without human involvement, which is a higher-risk use of ADMT. The definition of ADMT is necessary to provide clarity for businesses so that they can determine whether their use of technology substantially replaces human decisionmaking and is therefore in scope of the definition of "ADMT." These requirements are consistent with other privacy frameworks and California law, and align with efforts by Governor Newsom and the Legislature.
7001(e)	103	Comment appreciates the new definition of ADMT as technology that either replaces or substantially replaces human decision-making. Narrowing this definition creates a more workable threshold for companies to implement the obligations created by the ADMT regulations, leading to greater certainty for both companies and consumers about which technologies are subject to heightened protections.	The Agency notes comment's support.
7001(e)	65, 129, 160, 200, 387, 390, 448, 449, 450, 518, 547, 548	Comment appreciates removing subjective language from the definition but finds the "human involvement" requirement too vague. Comment requests clarification of the ADMT definition to ensure the regulation remains targeted, operationally feasible, and consistent with risk-based frameworks adopted in other jurisdictions. Comment proposes changes to vague language, such as replacing "relevant" with "necessary" as relevance is a subjective determination that will be implemented inconsistently by businesses. In addition, if interpreted expansively, requiring review of any and all "relevant" information may prove impossible for a human reviewer. A more workable approach would focus on whether the reviewer is equipped	The Agency disagrees with this comment. The regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. The comment's suggestion to change "relevant" to "necessary" in the definition is not more effective or appropriate at protecting consumer privacy in the context of ADMT. The regulation is meant to apply to many factual situations and across industries, and it is clear that the human reviewer is not required to review and analyze "all" information. The Agency has determined that no further clarification is needed at this time. Additionally, the Agency disagrees with the comment's suggestion to remove the language regarding replacement of

		with the knowledge to analyze outputs when appropriate rather than mandating review of each individual result. If a business has a protocol on what information is needed to make a decision or exception that should be sufficient. The Agency should also remove language on the replacement of human decisionmaking. Keeping this language removes the purpose of the exception. If a company were to make a decision based solely on a calculator, while perhaps not advisable, it should not be within scope. The Agency should expand the list of excluded tools to include other low-risk, operationally essential technologies, and clarify that profiling qualifies as ADMT only when it is used to make decisions about individuals without meaningful human involvement. The Agency should also include "search term software" to help limit unintentional capture of non-related technologies and actions. This would exclude when recruiters or employers conduct manual searches using terms to narrow the scope of a recruitment pool. Covering this step in the evaluation process will ensure that this activity is not brought in scope and subject to risk assessments and the suite of consumer rights that are ill-tailored to this employment context.	human decisionmaking from the exception; that language is necessary to ensure that businesses do not circumvent the ADMT requirements if one of the tools listed replaces human decisionmaking for a significant decision. The regulations balance protections for consumers' privacy and flexibility for businesses. The Agency also disagrees with including "search term software" in the exceptions as it is not clear what this software would include. Further, if a business were using search term software without human involvement to make a significant decision, the ADMT requirements would apply. Doing otherwise would be less effective at protecting consumer privacy.
7001(e)	159	Comment argues that the revised definition still reaches into areas that are the subject of active legislative consideration and executive policy development. Comment believes that the Agency should not regulate tools that still involve human involvement, and urges the Agency to reconsider the inclusion of ADMT regulations at this time.	The Agency disagrees with this comment. The regulations are issued pursuant to the CCPA's delegation of authority to the Agency. (*See* Civ. Code §§ 1798.185(a)(15), (b), 1798.199.40(b).) The regulations address the use of ADMT without human involvement, which is a higher-risk use of ADMT. They also provide a clear definition of ADMT and what constitutes human involvement. In addition, the Agency notes that it has engaged in robust preliminary rulemaking activities with a wide variety of stakeholders. The Agency looks forward to continuing to work with stakeholders, including the Legislature and Governor Newsom, on future policy development.

7001(e)	203, 210	Comment supports the revised definition of ADMT and the clarification of "substantially replace human decisionmaking." These changes promote regulatory focus on systems that warrant the most scrutiny, consistent with the risk-based principles reflected in the statute: technologies that operate without human oversight.	The Agency notes comment's support.
7001(e)	349, 350, 351	Comment argues that the revision of ADMT from "substantially facilitate" to "substantially replace" human decision-making significantly weakens the rule. The change implies that any automated decision-making process that includes the bare minimum of human involvement is somehow free from risk. The presence of human oversight has not prevented these systematic patterns of bias from occurring. In practice, many automated systems are deployed in emerging use cases where established expertise may not exist or are overseen by personnel who lack the specialized knowledge required to effectively audit algorithmic outputs. Furthermore, as AI becomes the new workplace standard, the risk for automation bias grows. Combatting automation bias requires deliberate product design, decision-making transparency, and reasonable guidelines about the volume of tasks that the users are expected to complete. The regulations offer developers no mandate to implement these components into their ADMT. With only the vague definition of "human involvement" in § 7001, companies are given immense discretion as to what bare minimum human involvement can look like. In the event that the Agency retains this definition of ADMT, comment urges the Agency to develop a more rigorous definition of "human involvement" that accounts for and mitigates the well-documented risks of automation bias. The regulation should require that human reviewers have sufficient resources, and time, in addition to authority, to meaningfully review automated decisions. The Board should incorporate this language requiring that human	The Agency disagrees with this comment. The definition of ADMT, including the definition of "human involvement," is clear and does not allow businesses to side-step accountability. Rather, it provides a clear performance-based standard that addresses a higher-risk use of ADMT. A business cannot self-certify out of coverage if it is using ADMT as set forth in the regulations, as doing so would violate the CCPA. With respect to bias, existing laws prohibit businesses from engaging in unlawful discrimination, which includes using ADMT for such purpose. The regulations also support the prevention of unlawful discrimination, such as by including the identification of this negative privacy impact and relevant safeguards in the risk assessment requirements. Further, the regulations require a human reviewer analyze the technology's output, which includes devoting the necessary time and resources to complete that requirement. This provision already addresses comment's concerns about lack of resources and time.

		involvement be substantive, not merely procedural. Comment suggests changes as follows: (2) Human involvement requires the human reviewer to: (A) Know how to interpret and use the technology's output to make the decision; (B) Review and analyze the output of the technology, and any other information that is relevant to make or change the decision, including a thorough description of the technologies' decisionmaking logic provided by the developer; and (C) Have sufficient authority, resources, and time to make or change the decision based on their analysis in subsection (B).	
7001(e)	372	Comment supports the revisions that narrow the definition of ADMT to tools that replace or substantially replace human decision-making. Comment also appreciates the addition of "without human involvement" in the definition of "substantially replace human decisionmaking," which aligns with the approach taken by other states and the federal government in establishing similar thresholds, such as the concept of "principal basis." On balance, these changes help ensure that the regulations squarely consider the extent to which ADMT outputs influence human-decision-making, which is a critical element in any effective risk-based approach. As a result, the scope of the ADMT regulations is more appropriately focused on those applications of ADMT that generally operate without a human in the loop and therefore pose potentially greater risks. This revised scope also better aligns California's privacy framework with other state privacy laws, which generally only govern fully or substantially automated decisionmaking technologies.	The Agency agrees with this comment to the extent that it supports the Agency's regulations and notes the comment's support.
7001(e)	389	Comment states that the definition could cover emerging agentic AI systems that automate routine business functions. This is overly broad because the tools are not "consequential decisions" as intended by the Agency and	The Agency disagrees with this comment. To the extent a business is using these tools as ADMT to make a significant decision about a consumer, it is subject to the corresponding risk assessment and Pre-use Notice, opt-out of ADMT, and access

		should not be subject to the same regulatory burdens as systems used for lending, hiring, or housing determinations.	ADMT requirements. The Agency does not believe that the definition is overly broad or would encompass low-risk uses of technology.
7001(e), 7001(ddd)	18, 23, 274, 278, 286, 465, 580	Comment argues that the revised definitions of "ADMT" and "significant decision" narrow the scope of regulation to such a degree as to render them meaningless to many Californians. This could allow many influential systems to escape oversight simply because they involve minimal human involvement. This is the same strategy businesses have adopted to circumvent New York City's algorithmic transparency law, Local Law 144, concerning automated decision technology used in employment decisions. The definition should be broadened to cover systems where the system is used to assist or replace human decisionmaking, even if the system does not make the final call. Covering circumstances where both a human and ADMT are involved in a decisionmaking process is essential because research shows humans tend to over-rely on automated systems. Alternatively, the definition should be broadened to cover where human users heavily rely on ADMT outputs. For workers in particular, the narrowing of scope to only automating uses of ADMT creates a large opening for companies to side-step the accountability that the Agency was charged with developing through its regulations. The definition of ADMT, which by statute must include instances where people's behavior and performance at work are predicted, falls short of that proper scope. ADMTs are one of the main ways that businesses use consumer and worker data, and so the numerous deletions and weakening of ADMT provisions in the revised regulations are especially harmful. Comment suggests reinstating the original definition proposed in summer 2023 and aligning it with the GDPR. Comment argues that the revised definition of ADMT allows companies to self-certify that they should not be subject to regulation: it explicitly carves out ADMTs where a	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT, including profiling. (*See* Civ. Code § 1798.185(a)(15).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) The ADMT definition, both as proposed and revised, is within the Agency's authority and furthers the intent and purpose of the CCPA. The regulations focus on businesses' use of ADMT without human involvement for significant decisions. They provide additional clarity for businesses and further simplify implementation for businesses at this time. The definition of ADMT, including the definition of "human involvement," is clear about what is required, and does not allow businesses to side-step accountability or self-certify out of coverage. Rather, the definition provides a clear performance-based standard that addresses a higher-risk use of ADMT. The definitions of ADMT and significant decision are necessary to provide clarity for businesses so that they can determine whether their use of technology for certain purposes is in scope of the regulations. The regulations continue to provide protections to workers, which includes requiring a risk assessment for certain automated processing in the workplace and for uses of ADMT for significant decisions, and requiring businesses to provide workers with a Pre-use Notice and opt-out of ADMT and access ADMT rights when a business plans to use ADMT for a significant decision. To the extent that a business is evaluating a person's behavior and performance at work using ADMT and using that ADMT to make a significant decision about them, the business must comply with Article 11's opt-out and access requirements. With respect to risk assessments, the CCPA requires risk assessments to be submitted to the Agency. As with

		human has even glancing involvement in making the decision. Under this new narrower standard, many more consumers will be denied the notice and opt-out protections they need and deserve. Also, without public access to risk assessments or required submissions to the Agency, enforcement will be limited.	other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law.
7001(e), 7001(ddd)	346	Comment requests that the definitions of "significant decision" and "automated decisionmaking technology" be narrowed to cover only truly high-risk decisions that pose a real threat to consumer privacy and exclude scenarios in which a human has oversight over the decision. For example, "significant decision" should be properly scoped as a decision that has a legal or material effect on an individual's life, such as approving or denying a home loan, and that poses a significant risk to consumer privacy. "Automated decisionmaking technology" should, as the name says, be focused on decisionmaking that occurs without human involvement or oversight. Day-to-day decisions about contract work are not, and should not count as, significant.	The Agency disagrees with this comment. The definition of ADMT focuses on decisionmaking without human involvement, as set forth in § 7001(e), which is a higher-risk use of ADMT. Similarly, the definition of significant decision addresses consequential decisions for consumers and provides clarity about what decisions are in scope. Further, it is unclear what "contract work" decisions the comment is concerned about. To the extent the comment is suggesting that decisions affecting independent contracting should not be in scope of the definition of significant decision, the Agency disagrees. The CCPA specifically includes independent contractors within its scope and provides them with privacy protections. (*See, e.g.,* Civ. Code § 1798.125(a)(1)(E).) The regulations implement these protections by ensuring that consumers subject to the use of ADMT for decisions regarding independent contracting opportunities and compensation are provided privacy protections.
7001(e), 7001(ddd)	487	Comment commends the Agency for refining key definitions and aligning obligations with a risk-based framework, especially the definitions of "ADMT" (§ 7001(e)) and "significant decision" (§ 7001(ddd)). The exclusion of advertising from significant decisions is especially helpful. Comment sees these changes as advancing the Agency's mandate while reducing unnecessary regulatory burdens.	The Agency notes the comment's support.
Previous 7001(g)	287	Comment urges the Agency to retain a clear definition of behavioral advertising. This is a critical and widely used	The Agency disagrees with this comment. The Agency revised the regulations to remove the profiling for behavioral advertising thresholds from Articles 10 and 11 to simplify implementation

		application of personal data that should not be left ambiguous.	for businesses at this time, and accordingly removed the definition of behavioral advertising. The Agency will continue to monitor the marketplace to determine whether modifications to the regulations are necessary.
7001(j)	190	Comment recommends deleting "annual" in § 7001(j).	The Agency disagrees with this comment. The definition aligns with the CCPA's direction to the Agency and with the requirements of Article 9. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to "perform a cybersecurity audit on an annual basis," with the regulations "establish[ing] a process to ensure that audits are thorough and independent." (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7001(*l*)	364	Comment supports distinguishing the definition of Cybersecurity Audit Reports separately from the audits themselves. Comment also supports that only the report be provided to executive management. These revisions match real-world audit practices and enable a more transparent audit process.	The Agency agrees with this comment to the extent that it supports the Agency's regulations, and notes comment's support.
Previous 7001(n)	288	Comment suggests that a clear definition of "deepfake" should remain in the rule to help identify this growing area of risk.	The Agency disagrees with this comment. The Agency revised the regulations to remove the "generation of a deepfake" thresholds from Articles 10 and 11 to simplify implementation for businesses at this time, and accordingly removed the definition of deepfake. The Agency will continue to monitor the marketplace to determine whether modifications to the regulations are necessary.
7001(t)	296, 326	Comment recommends revising the definition of "information system" to align more clearly with FTC GLBA Safeguards and New York State Department of Financial Services' definitions, and recommends specifying electronic resources. Comment requests clarification of what is meant	The Agency disagrees with this comment. The definition in the regulations is informed by, and is aligned with, others' definitions of the term, including the National Institute of Standards and Technology and the New York State Department of Financial Services. The definition is similarly aligned with the definition in the GLBA Safeguards Rule. The definition already covers

		by "resources" under § 7001(t) and recommends clarifying if the intent is to cover electronic systems.	electronic information resources. Regarding "resources," the regulation is reasonably clear based on the plain meaning of the word. The Agency believes that no further clarification is needed at this time.
7001(v)	63	Comment argues that the regulations would update the definition of "nonbusiness," subsequently creating confusion regarding the scope of the CCPA's applicability to nonprofits. The Agency should ensure that the regulations align with the CCPA by incorporating text that clearly limits its applicability to nonprofits.	The Agency disagrees with this comment. The revision aligns the regulation with the text of the CCPA. Civil Code § 1798.140(d)(2) defines "business" to include non-profits that control or are controlled by a business that share common branding with the business and with whom the business shares consumer personal information.
7001(bb)	496	Comment suggests that the Agency should align the definition of "penetration testing" (§ 7001(bb)) with the most current definition provided by the U.S. National Institute of Standards and Technology (NIST). This modification would foster interoperability with other data privacy and security rules and standards, consistent with the CCPA's instruction to "cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections."	The Agency agrees with this comment to the extent that it supports aligning with other privacy and security laws and existing standards when appropriate. The regulations' definition of "penetration testing" is informed by other regulators' definitions and descriptions of this term, such as the FTC and NYDFS, and is already aligned with NIST definitions. (*See, e.g.*, NIST SP 800-53, Rev. 5.) The Agency believes that modification is not needed at this time.
7001(ee)	7	Comment urges the Agency to separately define "profiling" and "physical or biological identification" as they are distinct concepts with different privacy implications. Profiling is inherently predictive and evaluative, focusing on behavioral, economic, or personal traits rather than direct physical or biological measurements. On the contrary, the definition of "physical or biological identification" serves to uniquely distinguish or confirm a specific person, typically by comparing captured data against a stored template or reference record. This process does not include predictive analysis or evaluation of personal aspects unrelated to identity confirmation.	The Agency disagrees with this comment. The comment's recommendation to separate the definitions is not necessary and is no more effective or appropriate than the regulation adopted by the Agency. The definition of "physical or biological identification or profiling" is clear and applies to both identification and profiling. It is unclear why separating the definition would be necessary to make it clearer.

7001(ee)	162	Comment urges removal of the definition of "physical or biological identification or profiling" due to overlap with the CCPA's existing definition of biometric data. Comment argues that the overlap could lead to confusion over when multiple assessments are required for a single activity and introduce unnecessary operational burdens.	The Agency disagrees with this comment. The training threshold, which includes the term "physical or biological identification or profiling," is distinct from the sensitive personal information threshold for risk assessments. The thresholds for conducting a risk assessment for training and for processing biometric information are not duplicative. For example, automated analysis of a consumer's facial expressions may not involve biometric information. In addition, to the extent that these thresholds overlap for a single processing activity, the regulations do not pose undue burden on businesses because they are only required to conduct a single risk assessment. (*See* § 7156(a)).
7001(ee)	325	Comment requests clarification on the term "automated" within § 7001(ee), as it is not defined.	The Agency disagrees with this comment. The regulation is reasonably clear based on the plain meaning of the word. The Agency believes that no further clarification is needed at this time.
7001(ee), 7150(b)	279	Comment opposes that the revised rules narrow the definition of "physical or biological identification or profiling." Comment believes that this makes three problematic changes to the risk assessment requirements with respect to profiling. The general risk assessment requirements now apply to profiling based on observation of people in sensitive locations but not in retail or other publicly accessible spaces; they now apply when a business intentionally processes personal data to train a technology that conducts physical or biological identification or profiling, but not when a business uses but does not train such technology; and additional risk assessment requirements specific to the use of physical or biological identification or profiling for significant decisions were removed. Businesses that deploy technologies off the shelf that enable physical or biological profiling could avoid performing risk assessments that capture how their specific uses of such technologies cause consumers to be targeted unfairly.	The Agency disagrees with this comment. The Agency revised the definition of "physical or biological identification or profiling" to provide additional clarity for businesses regarding which processing is in scope. In addition, the Agency revised the risk assessment thresholds and requirements to balance providing privacy protections for consumers with flexibility for businesses to come into compliance at this time. Further, businesses cannot avoid conducting risk assessments if their processing meets any of the thresholds in § 7150(b), and for these activities, they must identify privacy risks to consumers.

7001(ee), 7001(eee), 7150(b)(6)	455, 497, 522, 544	Comment suggests narrowing the language in § 7150(b)(6). The current phrasing captures too many low-risk models. Risk assessments should not be required for non-biometric training data. Comment argues that while they agree that emotion detection systems should be subject to risk assessment obligations when used to make significant decisions such as related to employment (as the example set forth in § 7150(c)(1) contemplates) or to identify consumers, there is no basis to require such an assessment when technology is not used for such purposes and the definition of "physical or biological identification or profiling" should be correspondingly narrowed. Comment suggests clarifying changes to align the regulations with legislative intent and similar privacy frameworks. Comment asks to clarify that § 7150(b)(6) and § 7001(ee) exclude non-identifying, non-significant-decision uses, and to delete "or profiling" in § 7001(eee). Comment further suggests that "physical or biological identification or profiling" at § 7001(ee) should be further tailored by introducing an intent standard, so that the obligations apply to systems intended to be used to identify individuals and exclude systems not used for identification purposes. The intent requirement should consider whether developers and deployers of biometric technologies take reasonable measures (e.g., technical, organizational, and contractual) to ensure that the processing of biometric characteristics cannot be used for identifying purposes. Adding this intent standard would align this definition with the statutory definition of "biometric information," where data is in scope if it is "is used or is intended to be used" for identification.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment. (*See* Civ. Code § 1798.185(a)(14)(B).) The training uses of consumers' personal information set forth in § 7150(b)(6), including training emotion recognition systems, pose significant risk to consumers' privacy. These risks include data leakage that can reidentify consumers whose personal information was used to train the model and a lack of transparency and consumer control over the use of their personal information for training. These risks extend to non-biometric information as well. Comment's suggested language is also less effective than the regulation because it would exclude training uses of personal information for profiling.
7001(ii)	161	Comment expresses concern that the definition of "profiling" is too broad and imposes regulatory requirements on all automated analysis, regardless of whether it results in meaningful consequences for individuals. Comment suggests that the definition of	The Agency disagrees with this comment. The comment misinterprets the plain language of the regulation. The definition of "profiling" alone does not impose regulatory requirements on businesses. The risk-assessment and ADMT articles impose regulatory requirements on businesses that use ADMT for

		profiling should be narrowed to exclude systems used for public safety, physical security, and fraud prevention.	significant decisions. (*See* §§ 7150(b)(3), 7200(a).) In addition, certain training uses for physical or biological identification or profiling are subject to risk assessment requirements. (*See* § 7150(b)(6).) The regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. Further, additional exclusions are not necessary. The current exceptions in Article 11 appropriately balance ensuring consumers can exercise their CCPA rights to opt-out of ADMT and access ADMT with appropriate protections for certain information related to safety, security, and fraud prevention in §§ 7220(d)(2) and 7222(c)(2).
7001(ii)	495	Comment states that the concept of "automated processing" appears several times throughout the modified rules and is important in the definition of profiling (§7001(ii)) as well as the rules for determining when a risk assessment must be completed (§§ 7150(b)(4), (b)(5)). The phrase appears intended to address instances where processing is solely automated. The text should clarify this scope accordingly.	The Agency disagrees with this comment. The term "profiling" is not limited to solely automated processing, and the Agency believes that no further clarification is needed at this time.
7001(ii), 7024(e)	202	Comment asserts that there are still issues with the scope of the regulations related to the definition of profiling at § 7001(ii) and burdensome information-sharing requirements under the right to know at § 7024(e); the Agency should tailor these areas to ensure workability and reasonability. Comment indicates that it is aligned with the California Chamber of Commerce's comments.	The Agency disagrees with this comment. The definition of "profiling" does not impose regulatory requirements on businesses. The risk-assessment and ADMT articles impose regulatory requirements on businesses that use ADMT for significant decisions. (*See* §§ 7150(b)(3), 7200(a).) In addition, certain training uses for physical or biological identification or profiling are subject to risk assessment requirements. (*See* § 7150(b)(6).) The regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. Regarding the comment's concerns about § 7024(e), the modifications the Agency made actually simplify the requirements in responding to consumers' requests by removing the requirement to inform

			consumers that they can file a complaint with the Agency or the Attorney General's office. With its removal, the regulation does not impose additional obligations on businesses and instead provides additional clarity. Further, it is unclear what the comment is recommending with respect to aligning itself with the California Chamber of Commerce's comments.
7001(pp)	391	Comment proposes excluding first-party advertising from the definition of "request to opt-in to sale/sharing" and amending to "the use of personal information for first-party advertising does not constitute a 'request to opt-in to sale/sharing' and does not require separate consent."	The Agency disagrees with this comment. The comment's proposed change to the definition is unnecessary and would be confusing. The request to opt-in to sale/sharing definition applies to "sale" or "sharing" of personal information, which by definition applies to the disclosure or making available of personal information to third parties.
7001(aaa), 7150(b)(5)	76, 163, 181	Comment asserts that the Agency does not have carte blanche authority to issue new regulations on sensitive locations. Expanding regulatory authority in this way violates fundamental principles of administrative law. Any expansion of covered data categories must come from the Legislature, not through agency rulemaking. References to sensitive locations must be removed from the text. Introducing "sensitive location" as a distinct concept imposes new risk assessment obligations based not on the nature of the personal information, but on the location where a person happens to be. § 7150(b)(5) would require risk assessments for the use of automated processing to infer consumer traits based on their presence at such locations. This expands the scope of regulated conduct far beyond what the statute permits and introduces substantial compliance burdens without clear statutory justification. This is already addressed by the sensitive personal information threshold, which undermines the statutory structure and creates legal uncertainty.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring risk assessments for processing of personal information that presents significant risk to consumers' privacy. (*See* Civ. Code § 1798.185(a)(14)(B).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) Automated processing of consumers' personal information to develop certain inferences and extrapolations about consumers, based on their presence in a sensitive location, is within this authority. The definition is necessary to provide clarity to businesses and consumers about what locations are subject to certain requirements. § 7150(b)(5) is necessary to provide clarity to businesses regarding what personal information is subject to this threshold. This is distinct from the "processing sensitive personal information" threshold at § 7150(b)(2). To the extent these thresholds overlap for a single processing activity, it does not pose undue burden on businesses because they are only required to conduct a single risk assessment for that activity. (*See* § 7156(a).)
7001(aaa)	436, 437	Comment supports requiring risk assessments when businesses associate consumers with sensitive locations,	The Agency notes comment's support but otherwise disagrees with this comment. The locations identified as sensitive are not

		but recommends that the Agency amend the definition of to align it more closely with the NAI's existing definition of "sensitive POIs" and FTC precedent. Comment believes that the change would tailor the definition more closely to risks of harm as the definition is both too broad when it includes locations that are not likely to increase the risk of harm; and incomplete when it omits categories of locations that may pose those risks. Comment believes that aligning the definition with the NAI's definition of sensitive POIs will promote uniformity and help businesses adopt a common standard for when a location or other point of interest is sensitive.	overly broad but address places that present heightened privacy risks for consumers. The Agency will continue to monitor the marketplace to assess whether additional locations should be added.
7001(aaa)	468	Comment criticizes the regulation that narrows public profiling to only "sensitive locations." This new construction leaves out the profiling of consumers in other public spaces—such as retail businesses, streets, entertainment venues, or public transit—from the risk assessment requirements. Profiling in such public, non-sensitive spaces still threaten consumer privacy.	The Agency disagrees with this comment to the extent it suggests modifications to the regulations. The Agency revised the risk assessment thresholds and requirements to balance providing privacy protections for consumers with flexibility for businesses to come into compliance at this time.
7001(bbb)	256	Comment opposes expanding the definition of sensitive personal information ("SPI") to include minors' data. Such a change effectively alters statutory definitions and should be pursued, if at all, through legislation.	The Agency disagrees with this comment. Civil Code § 1798.185(a)(1) clearly gives the Agency authority to add categories of sensitive personal information. The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) Adding minors' personal information to the definition of SPI aligns the definition with several other jurisdictions while also reflecting how California's law gives additional protections to consumers 13 to 15 years of age.
7001(ddd)	54	Comment asks the Agency to clarify the definition of "significant decision" so that it applies solely to decisions about consumers acting in individual or household contexts and not in commercial or business to business contexts. Furthermore, definitions related to rights to opt out of and	The Agency disagrees with this comment. The significant decision definition explicitly extends into business contexts, such as with respect to employees, independent contractors, and sole proprietorships. The comment's suggestion to narrow the scope of the definition would not be more effective, and would be less

		access ADMT should clearly indicate that they apply solely to the use of ADMT for significant decisions. While definitions of key terms, such as "right to opt-out of ADMT," "request to opt-out of ADMT," "right to access ADMT," and "request to access ADMT" apply "as set forth in . . . Article 11," which creates requirements for use of ADMT for significant decisions, to foster clarity, the definitions should be revised to explicitly state that they pertain exclusively to ADMT within the context of significant decision-making. Such a clarification would help to squarely limit the impact of new rights to use of ADMT for significant decisions and avoid the potential for scope creep.	protective of consumers' privacy. In addition, the comment's recommendations to add the term "significant decision" to other definitions is unnecessary. The ADMT requirements in Article 11 are already limited to a business's use of ADMT for significant decisions at this time, so it would be redundant to add the term "significant decision" to the definition of ADMT. It is unclear what the comment means by "scope creep." The regulations are both within the Agency's authority and consistent with the intent and purpose of the CCPA.
7001(ddd)	66	Comment appreciates the clarification of what constitutes a "significant decision," which now focuses on high-impact decisions and excludes routine or preparatory steps. This improves both the clarity and practicality of the rules.	The Agency notes commenter's support.
7001(ddd)	105, 108, 177, 311, 338, 379, 393, 456, 488, 490, 491 519, 549	Comment appreciates narrowing the definition of significant decision. However, comment raises concerns that the definition is still overly broad and covers immaterial or trivial conduct, including employment-related decisions and healthcare services. For example, the definition of "healthcare services" could cover automated scheduling of gym sessions; inclusion of benefits for employees could include gift cards and discounts; and inclusion of allocation or assignment of work, per-assignment compensation, or incentive compensation could include minor decisions. Comment suggests binding the language on compensation to focus on decisions with material adverse legal or economic effects and excluding activities that do not meet this threshold, such as routine administrative actions needed to process payroll. § 7001(ddd)(1)-(6) should be further narrowed, including removing "allocation or assignment of work" and "employment or independent contracting opportunities or	The Agency disagrees with this comment. The definition is not overly broad. The CCPA specifically includes employees and independent contractors within its scope and explicitly provides them with privacy protections. In addition, the definition is consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about which decisions are in scope. It does not conflict with CRD's regulations nor with efforts by the Legislature. The comment's suggestions would not be as effective in providing that clarity for businesses. Moreover, the Agency determined that a business's use of ADMT for employment decisions, including to allocate or assign work and compensation, presents significant risk to consumers' privacy and accordingly retained those decisions in the definition of "significant decision," and requires businesses to conduct a risk assessment before initiating such processing. Allocation or assignment of compensation is a significant decision and does not require additional clarification. It is unclear what the

		compensation." These are routine business operations, they encompass a broad range of activities, and they do not present high privacy risks. Regulating them could hamstring routine operations, risk conflicts with California Civil Rights Department's ("CRD") and the Legislature's ongoing efforts to regulate ADMT in the workplace, and risk confusing consumers. Including them will also create compliance burdens without proportional consumer benefit. Comment states this burden is the type of over-inclusion identified by Governor Newsom in his April letter. The definition should be revised to state: "An action is not a 'significant decision' if it does not have a material, legal, or similarly significant effect on a consumer." Or, it can be revised as follows: (1) adding the following language to § 7001(ddd): "'Significant decision' means a decision that results in a material or similarly significant effect on the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services," and (2) revising § 7001(ddd)(4)(B) as follows: "'Employment or independent contracting opportunities or compensation' means: (A) Hiring; (B) For employees, assignments that materially impact hiring, promotion or compensation; or salary, wage, or bonuses; (C) Promotion; and (D) Demotion, suspension, and termination." Comment alternatively recommends aligning with EU AI Act language that focuses on allocation of tasks based on individual behavior or personal traits or characteristics. This approach is more appropriately targeted to the subset of allocation/assignment use cases that could pose risks to consumers, while retaining the apparent policy objective in the regulations. Comment also recommends not requiring risk assessments for a business's use of ADMT for employment decisions.	comment means by "routine administrative actions"; to the extent that these are uses of ADMT that allocate or assign consumers' compensation, they are in scope. The definition of healthcare services is clear and does not encompass low-risk activities.

7001(ddd)	130, 232, 253, 319, 321, 324	Comment supports inclusion of hiring and firing of employees in "significant decision" but urges to limit it to the hiring and firing of employees. The Agency should focus its ADMT provisions only on material employment-related decisions, like hiring, promotion, and termination, or high-risk decisions that materially affect individuals' privacy rights. It should avoid regulating day-to-day business processes that support the functionality, convenience, and efficiency of services Californians use every day. In particular, the rules propose a broad definition of "employment or independent contracting opportunities or compensation" decisions that would include any tool used to allocate or assign work. Comment opposes the inclusion of "allocation or assignment of work" and "per-assignment compensation" in the definition of "significant decision." Including "allocation or assignment of work for employees" could be interpreted to include routine task routing tools, such as call center queue systems. By striking "allocation or assignment of work" and "per-assignment compensation" from the definition of "significant decision," the Agency can strike a balance to protect consumer privacy while avoiding burdens on the tools that make these services work. Alternatively, if the Agency chooses to retain these categories, comment recommends narrowing their scope to apply only within the traditional employer-employee context and not to independent contractors.	The Agency disagrees with this comment. In revising § 7001(ddd)(4), the Agency considered the types of decisions that have important consequences for consumers and present significant risk to their privacy and determined that all of the following meet those criteria: hiring; allocation or assignment of work for employees; salary, hourly or per-assignment compensation, incentive compensation such as a bonus, or another benefit; promotion; and demotion, suspension, and termination. The regulations balance protecting consumers' privacy and simplifying implementation for businesses as this time. The comment's suggestion to further narrow § 7001(ddd)(4) is no more effective or appropriate than the regulation adopted by the Agency. The Agency will continue to monitor the marketplace to determine whether modifications to the regulations are necessary.
7001(ddd)	208, 320	Comment criticizes the ADMT regulations for defining "significant decision" too broadly, such as the inclusion of "allocation or assignment of work for employees" or "per-assignment compensation." Comment argues that platform companies like Uber, DoorDash, and Instacart use algorithmic tools to assign tasks in their normal course of business. These are not "significant decisions" in the sense of granting or denying employment, or determining an annual bonus. These rules would harm platform economy,	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) The ADMT regulations and the definition of significant decision, both as proposed and revised, are within the Agency's authority

		burdening not just tech companies but also workers, consumers, and small businesses. The scope extends the rule's reach to business decisions that do not raise meaningful privacy concerns. Applying the same regulatory requirements to these everyday processes as would apply to high-risk decisions like access to credit or health care decisions risks expanding the Agency's scope into areas outside of its core privacy objectives, which could inadvertently divert attention from its efforts and dilute the impact the Agency can make. Comment appreciates Board Member Mactaggart's recognition of widespread concerns about regulatory overreach and lack of statutory grounding. Comment narrows their comments to specific concerns in relation to the management of independent contractors and other decisions they believe to be significant.	and further the intent and purpose of the CCPA. The regulations are necessary to address businesses' use of ADMT without human involvement for significant decisions, and the definition of significant decision is necessary to provide clarity for businesses. In revising the regulations, the Agency considered the types of decisions that have important consequences for consumers and present significant risk to their privacy. The Agency determined that a business's use of ADMT to allocate or assign work for employees presents significant risk to consumers' privacy and accordingly retained it in the definition of significant decision. The comment's suggestions to narrow the definition of significant decision is no more effective or appropriate than the regulation adopted by the Agency. The Agency has made efforts to limit the burden of the regulation while implementing the CCPA. The regulation balances protecting consumers' privacy with simplifying implementation for businesses as this time.
7001(ddd)	90, 213	Comment raises concerns that the ADMT regulations may unintentionally interfere with commercial credit reporting. The use of business-related personal data in credit reports could be misclassified under ADMT opt-out provisions, which could negatively affect businesses and service providers, including small businesses. Comment proposes adding language to explicitly exclude commercial credit reporting from the definition of "significant decision" in the ADMT rules. Comment proposes amending (ddd)(7) to state: "A significant decision does not include the purposes set forth in Section 1798.145(o)." This exemption would support the availability of credit to California businesses.	The Agency disagrees with this comment. The CCPA's statutory exemptions already apply to the regulations, and the Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations do not impede California businesses' access to credit. To the extent these businesses are subject to the regulations, the regulations ensure transparency when ADMT is used to make significant decisions without human involvement.
7001(ddd)	164, 214, 231, 252, 394, 492	Comment appreciates the narrowing of the "significant decision" definition but maintains it remains overly broad. Comment proposes that for the definition of "financial or lending services," the reference to "financial" should be removed or narrowed to align with other jurisdictions.	The Agency disagrees with this comment. The definition is not overly broad. To the extent the comment suggests that certain financial or lending services should be excluded because they are already regulated, the Agency notes that the CCPA is reasonably clear in addressing which businesses and data are subject to the

		Comment suggests limiting "financial and lending services" to a more clearly delineated set of high-risk activities, such as extension of credit or a loan. While the inclusion of decisions related to the extension of credit is more clearly tied to consumer impact, the remainder of the category sweeps in activities that are routine, already regulated, and not appropriately treated as "significant decisions." For example, they include routine and operational activities such as transmitting or exchanging funds and check cashing. They also bring in tools used for common purposes such as digital payments, and automated payments for bills or wage payment systems, as well as payment apps, money transfer features, and digital wallets. It may also include AI tools that companies use to comply with financial rules and regulations. The "provision" of deposit and checking accounts, transmitting funds, and facilitating installment payments may capture lower-risk processing to operate existing accounts. Such requirements would endanger the security of financial systems and also contradict the consumer protection goals of the CCPA. Comment recommends deleting the reference to "transmitting or exchanging funds" and refining the language around accounts to refer only to credit adjudication and the "opening" of deposit or checking accounts, rather than the broader and less precise term "provision." Greater clarity should also be provided as to how these obligations will work with respect to the GLBA exemptions specified in the law. Comment also argues that the inclusion of employment-related decisions that extend beyond hiring and termination raises significant issues. Comment recommends deleting § 7001(4)(B).	CCPA. All of the CCPA's exemptions apply to the regulations, and the Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, with respect to the definitions of "financial or lending service" and the definition in § 7001(ddd)(4)(B) of "employment or independent contracting opportunities or compensation," the Agency considered the types of decisions that have important consequences for consumers and present significant risk to their privacy and determined that all of the following meet those criteria: transmitting or exchanging funds, the provision of deposit or checking accounts, check cashing, and installment payment plans; allocation or assignment of work for employees; salary, hourly or per-assignment compensation and incentive compensation such as a bonus, or another benefit. The comment's suggestions to change "provision" to "opening" and to narrow the definition of "financial or lending services" are not more effective or appropriate than the regulation adopted by the Agency. Also, the regulations would not prevent a business from using tools for common purposes like digital payments, automated payments for bills, wage payment systems, or AI tools to comply with financial rules and regulations. To the extent these tools are subject to Article 11, a business would need to comply with the Pre-use Notice, opt-out of ADMT, and access ADMT requirements. Further, the CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal or state law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) The regulations would not endanger the security of financial systems and provide relevant exceptions for security, fraud prevention, and safety information as appropriate. The regulations are consistent with the CCPA's direction to the Agency, further the intent and purpose of the CCPA, and balance protecting consumers' privacy with simplifying implementation for businesses as this time.

7001(ddd)	269	Comment asserts that if the term "significant decision" continues to reference "financial or lending services," then many financial/lending tools may be considered ADMTs, and thus would require lenders to use older manual underwriting or fraud review methods that have not been frequently used, may be inaccurate, and impair the cost of credit.	To the extent the comment suggests the Agency should further narrow the definition of "significant decision," the Agency disagrees. In defining "financial or lending service," the Agency considered the types of decisions that have important consequences for consumers and present significant risk to their privacy, and determined that all of the following meet that criteria: transmitting or exchanging funds, the provision of deposit or checking accounts, check cashing, and installment payment plans. The regulations are consistent with the CCPA's direction to the Agency and further the intent and purpose of the CCPA. The comment does not provide evidence that the regulation would impair the cost of credit. Further, commenter seems to misunderstand the regulations as they do not prohibit businesses from using ADMT for significant decisions. Rather they require businesses to engage in a risk assessment, and provide consumers with a Pre-use Notice, the ability to opt-out of the business's use of that ADMT subject to certain exceptions, and the ability to access information about the use of ADMT. The regulations balance protections for consumers' privacy with simplifying implementation for businesses at this time.
7001(e), 7001(ddd)	297	Comment argues that the scope of the "significant decision" definition should be limited to businesses that are offering, or from which a consumer is seeking, such services. Comment raises concern that a business that furnishes information to credit reporting agencies could be considered to be making a significant decision if the information provided positively or negatively affects the consumer's credit score or the provision of financial or lending services by other businesses.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The CCPA does not exempt businesses that are not offering a service to a consumer or from which consumers are not seeking a service. With respect to furnishing information to consumer reporting agencies, the CCPA includes data-level exemptions for the processing of personal information by certain entities, as long as the activity is regulated by the FCRA and the processing is as authorized by the FCRA. (*See* Civ. Code § 1798.145(d).) The comment's suggestion to further narrow the definition is no more effective or appropriate than the regulation adopted by the Agency. The regulations balance protecting

			consumers' privacy with simplifying implementation for businesses as this time.
7001(ddd)	204	Comment urges the Agency to define "significant decision" to mean legal or similarly consequential determinations affecting consumers.	The Agency disagrees with this comment. The regulations provide more clarity for businesses as to which decisions are in scope than the comment's recommendation. Further, the definition is consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses.
7001(ddd)	374	Comment supports the revised definition of "significant decision" which is limited to the "provision or denial" of important benefits and services, while removing the broader "access to" language. The regulations target decisions with direct and material impact on consumers, which is an important element of an effective and nuanced risk-based approach. This change would also align California's regulations with every other state privacy law that governs similar decisions, which are limited to "provision or denial" only.	The Agency agrees with this comment to the extent that it supports the Agency's regulations and notes comment's support.
7001(ddd)	392	Comment states the definition of "significant decision" risks being beyond the statutory scope of the Agency's rulemaking.	The Agency disagrees with this comment. The CCPA directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment, and to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code §§ 1798.185(a)(14)(B), (a)(15).) The definition of "significant decision" is necessary to clarify the types of decisions that are in scope of these requirements.
7001(ddd)	275, 466, 582	Comment criticizes the narrowed scope of "significant decisions" and suggests reinstating the inclusion of "insurance," "criminal justice," and "essential goods or services" into the definition. Comment argues that the thresholds for risk assessment obligations are too high and will wrongly exclude ADMT uses that pose significant	The Agency disagrees with this comment. The Agency removed these terms to simplify implementation for businesses at this time. The regulations, as revised, continue to provide privacy protections for consumers, including with respect to the use of ADMT for a significant decision.

		privacy risks and undermine meaningful control over personal information.	
7001(ddd)(6)	353, 493	Comment proposes clarifying language in § 7001(ddd)(6) to ensure that regulated businesses are not discouraged from using critical cybersecurity technologies to safeguard the personal and sensitive data they possess. Specifically, comment recommends clarifying that a significant decision also does not include using technologies that combat cybersecurity threats by drafting § 7001(ddd)(6) to state the following: Significant decision does not include advertising to a consumer, detecting and preventing security incidents, and/or resisting malicious, deceptive, fraudulent, or illegal activity.	The Agency disagrees with this comment. To the extent a business is using ADMT to make a significant decision about a consumer, it must comply with the requirements in Articles 10 and 11. The regulations already include appropriate exceptions for security, fraud prevention, and safety. (*See* §§ 7220(d)(2), 7222(c)(2).) The comment's recommendation would be less effective at protecting consumer privacy, because it would limit the types of significant decisions for which businesses would be required to conduct risk assessments, and for which consumers would receive Pre-use Notices and the right to opt out of ADMT and access ADMT.
7001(eee), 7150(b)	157, 234, 235, 498	Comment argues that the Agency's rules would still require risk assessments for certain activities that do not present analogous risks to consumers. For example, the definition of "systematic observation" captures any "methodical and regular or continuous observation" of employees. This is a vague and seemingly overbroad trigger given that important information security, safety, and risk management principles require at least some regular observation of employees in the workplace. Comment suggests clarifying that "systematic observation" means methodical and regular or continuous observation, which includes methodical and regular or continuous observation using Wi-Fi or Bluetooth tracking, radio frequency identification, drones, video or audio surveillance (such a closed-circuit television) or live-streaming, technologies that enable physical or biological identification or profiling; and geofencing, location trackers, or license-plate recognition. These present a greater degree of risk than other types of recording (such as recording of business meetings). Comment also suggests that the threshold for conducting risk assessments should be aligned to existing	The Agency disagrees with this comment. The definition of "systematic observation" is clear and provides several examples as guidance to businesses regarding what is in scope. In addition, both this definition and the corresponding threshold in § 7150(b)(4) are tailored to address consumer harms from systematic observation in the workplace. Further, a risk assessment is consistent with the security, safety, and risk management principles that commenter cites to, and the risk assessment ensures that businesses identify relevant privacy risks and safeguards for this type of processing in the workplace. The regulations are consistent other privacy frameworks, such as the GDPR and the Colorado Privacy Act.

		risk assessment frameworks and other sections of the draft regulations.	
Previous 7001(kkk)	2	Comment is disappointed by the removal of Zero Trust Architecture ("ZTA") from the regulation and urges its reinstatement. Comment believes that ZTA is an important adjunct to multifactor authentication ("MFA")-based guidance, and other baseline identity measures, because it can stop attacks even if legitimate credentials are compromised and MFA is bypassed. Therefore, it is a constructive element of the regulation.	The Agency agrees with this comment's support for proactive cybersecurity measures. The Agency disagrees with the comment's suggestion to add "zero-trust architecture" at this time. The Agency deleted zero-trust architecture to simplify implementation at this time. However, the regulations are clear that an audit may assess and document components of a cybersecurity program that are explicitly not set forth in §§ 7123 (b) or (c), including ZTA. (*See* § 7123(d).)
7004	360	While supporting the intent of § 7004 prohibiting dark patterns, comment points out that many small and medium enterprises use third-party web or app platforms (e.g., Shopify, Wix, Squarespace) that limit their ability to control consent flows fully. The Agency should consider issuing UI/UX implementation templates for consent, ideally tailored for popular platforms and mobile contexts. This would empower small and medium size enterprises to meet legal expectations without incurring costly redevelopment. A "compliance kit" with open-source designs could significantly reduce violations due to lack of technical access or awareness.	The Agency notes the comment's support of the regulations. The Agency also notes the commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7004	499	Comment suggests that the symmetry in choice requirement in § 7004(a)(2)(A) should reflect that there may be a different number of steps needed for a consumer to opt in (e.g., through a single click) versus opt out of sharing information – which could, for example, necessitate follow-on verifications. The regulations should require symmetry as a general principle but not limit optouts to the "same or fewer" steps in all instances. The Agency should take care to ensure that the prohibition on "general or broad terms of use" (§ 7004(a)(4)(C)) within choice architecture is not in tension or conflict with the broader	The Agency disagrees with this comment, which misstates the law. Opting-out of the sale/sharing of personal information is not a verifiable consumer request under the CCPA. The business should not be requiring verification for requests to opt-out of the sale/sharing of personal information. The comment on § 7004(a)(4)(C) also appears to misunderstand the CCPA. Civil Code § 1798.140(h) defines "consent" to mean "any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer... signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose." The definition goes on to say, "[a]cceptance of a general or broad

		requirements of the law for business to provide a Notice at Collection.	terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent." The regulation is a restatement of the law in a way that makes it easier for businesses and consumers to understand. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.

ARTICLE 2. REQUIRED DISCLOSURES TO CONSUMERS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7010(d)	550	Comment seeks removal of this provision. Persistent opt-out links are not consumer friendly and real-time options are more appropriate. Businesses should have flexibility to determine interaction methods.	The Agency disagrees with this comment. The notice requirements in the regulations provide businesses with flexibility in how they are consolidated or included with the Notice at Collection. The Agency disagrees that the notice requirements would impede consumers, because these notices ensure that consumers have meaningful information prior to exercising their CCPA rights.
7013(e)(3)	62	Comment argues that the prescriptive requirements would limit businesses' ability to effectively reach consumers with notices across multiple channels in ways that are more accessible and consumer friendly. They also fail to acknowledge advancements in technology, which may not permit or may make it impractical to provide notices through the medium that actually collects personal information, such as AR/VR devices.	The Agency disagrees with this comment. The purpose of the Notice at Collection is to provide consumers with timely notice, at or before the point of collection, so that consumers have a tool to exercise meaningful control over the business's use of their personal information. The examples provided are clear and necessary to provide businesses with clarity on how to provide such notices. In the augmented or virtual reality setting, the notice must be given before or at the time the consumer encounters the business collecting the personal information. The regulations apply a performance-based standard that gives businesses flexibility to craft a method for providing notice as long as the consumer will encounter the notice before or at the time the device begins collecting the personal information.
Notices generally	289	Long-term services often rely on a single consent point, which may not be remembered or remain meaningful over time. For high-impact data uses,	The Agency agrees with this comment to the extent that it supports consumers being informed of their rights and the regulations' notice requirements. The Agency disagrees with this comment to the extent that it suggests that the Agency modify the regulations at this time. The

		periodic notices—like those in financial or educational contexts—should be required.	comment does not specify which notices should be periodic or how often. The CCPA already requires businesses to update their privacy policies once every 12 months. (*See* Civ. Code § 1798.135(a)(5).)

ARTICLE 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7020(e)	27	Comment appreciates clarity on time constraints in § 7020(e), but argues that requiring production of data back to January 1, 2022, is burdensome and incentivizes unnecessarily longer data retention. They propose limiting the look back period to January 1, 2024.	The Agency disagrees with this comment. The requirement to produce data back to January 1, 2022, is required by statute. (*See* Civ. Code § 1798.130(a)(2)(B).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Additionally, this regulation relates to the method offered by the business for the submission of requests to know. It does not require businesses to maintain personal information for longer than 12 months. (*See* Civ. Code § 1798.145(j)(2) [no CCPA requirement to retain any personal information about a consumer, if in the ordinary course of business, that information would not be retained].)
7020(e)	257	Comment expresses concerns with the change to § 7020(e), which effectively transforms a permissive statutory provision into a mandatory regulatory requirement. The regulation should clarify that responses are limited to information the business continues to maintain.	The Agency disagrees with this comment. This regulation relates to the method offered by the business for the submission of requests to know. It does not require businesses to maintain personal information for longer than 12 months. (*See* Civ. Code § 1798.145(j)(2) [no CCPA requirement to retain any personal information about a consumer, if in the ordinary course of business, that information would not be retained].) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. If business does not maintain the personal information at issue, there is no personal information that would be subject to the consumer's request.
7022	290	Comment argues that the rule should ensure that deleted or de-identified data remains that way and is not quietly reintroduced through subsequent data pulls. This is critical, especially in light of data broker practices.	The Agency disagrees with this comment to the extent that it contends that the regulations should be modified. The regulations already state that businesses must permanently and completely erase the personal information subject to the

			request in their systems. The Agency has determined that no additional language is necessary at this time.
7022	28	Comment supports the Agency's modifications to § 7022 ("Request to Delete"), as they will help ensure that all parties, including service providers and contractors, can more easily comply with the numerous provisions in the section.	The Agency agrees with this comment and notes commenter's support.
7023	254	Comment objects to the requirements for granular metadata tracking in §§ 7023(c), 7023(i), and 7023(k), which impose an unreasonably high burden on data management systems. These provisions would necessitate the tracking of individual data elements across all systems and compel businesses to maintain corrected information indefinitely and across all future data inputs.	The Agency disagrees with this comment. The regulations and examples provided benefit both consumers and businesses in ensuring that personal information maintained by the business is accurate and not overwritten by incorrect information, which would render the request obsolete. Businesses also benefit by having accurate information.
7020(e), 7023(c)	500	Comment recommends clarifications that according to the commenter would reduce unrealistic burdens on businesses, such as clarifying that response to requests to know only applies to data still retained and restoring "implement measures to" language in correction obligations to reflect practical limitations.	The Agency disagrees with this comment. The Agency does not think that the proposed language is necessary to clarify the regulation. § 7020(e) applies to requests to delete. If the business does not maintain the personal information at issue, there is no personal information that would be subject to the request to delete. As to § 7023(c), the regulation is reasonably clear, and the examples provided within the regulation already explain what is meant by the term "remains corrected."
7022, 7023	291	Comment suggests that consumers should continue to be informed of their right to file complaints with the Agency, unless a request has been determined to be fraudulent.	The Agency agrees with this comment to the extent that it supports consumers being informed of their ability to file complaints with the Agency. However, the Agency has removed provisions requiring businesses to inform consumers of their rights in its denial of requests to simplify implementation at this time. Information regarding the right to file complaints can still be found in the CCPA and on the Agency's website.

7025(c)	8, 9	Comment suggests strengthening references to pseudonymisation by adding the following language to both §§ 7025(c)(1) and (c)(2): "We recommend strong pseudonymisation techniques would be used, notably to avoid reverse-tracking & fingerprinting and to promote a secured user-centric approach".	This comment is not related to any modification to the text for the 15-day comment period. The Agency notes comment's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7025(c)	10	Comment believes that the example in § 7025(c)(7)(D) of Ramona's conflict between her opt-out signal and participation in Business P's financial incentive program highlights a critical flaw in current privacy choice architectures: fragmented, context-dependent controls that force users to manually reconcile conflicting preferences across systems. Comment recommends a solution with the product from their company.	The Agency disagrees with this comment, which appears to seek the Agency's approval of its consent management platform as a method for submitting CCPA requests and obtaining consent. The Agency has adopted a performance-based standard to provide businesses with flexibility to determine how to meet the requirement that best fits their business operations. The Agency has determined that it is not necessary to provide an example of a compliant consent management platform or require a specific product.
7027(m)	172	Comment argues that the example in § 7027(m)(2)(B) should better reflect the full range of legitimate purposes for scanning outgoing employee emails. Comment recommends deleting the second sentence of this provision or revising it.	The Agency disagrees with this comment. § 7027(m)(2)(B) is an example of a type of use of sensitive personal information that would fall within the listed exception to the right to limit. Examples do not need to reflect all instances in which a business may fall within this exception. The Agency has determined that no further clarification is needed at this time.
7027(m)	501	Comment suggests that the Agency should add language indicating that where illustrative examples are provided, such as under §§ 7023(m)(2) and (3), those examples are not meant be exhaustive.	There are no §§ 7023(m)(2) and (3), so the Agency assumes that the comment is referring to §§ 7027(m)(2) and (3). The Agency disagrees with this comment. It is not necessary to state that examples are not meant to be exhaustive because there is nothing in the text of the regulations that would indicate that they are supposed to be exhaustive.
7022(g)(5), 7023(f)(6), 7024(e)(3), 7026(e), 7027(f)	29	Comment supports the removal of the requirements throughout Article 3 to inform consumers that they can file a complaint with the Agency and the Attorney General.	The Agency agrees with this comment and notes commenter's support.

7025(c)(6), 7026(g), 7027(h)	61	Comment argues that the regulations would shift the current voluntary business disclosure of an opt out preference signal's status through an "Opt-Out Request Honored" disclosure into a mandatory requirement. This would be a significant burden on businesses, particularly small to mid-size firms. To maintain flexibility, the Agency should preserve the existing approach which allows businesses to decide whether or not to display this status.	The Agency disagrees with this comment. This regulation is necessary to avoid confusion for consumers about their opt-out status while using a business's website or online services. It gives consumers the ability to know that the signal is being consistently applied across the different websites they visit and engenders confidence in the opt-out preference signal preventing the sale or sharing of their personal information. The benefit of the regulation outweighs the cost to businesses.

ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7050(h)(2), 7153(a)	371, 503	Comment suggests that the Agency should further amend the language in §§ 7050(h)(2) and 7153(a) to prevent undue and unintended burdens on service providers. To efficiently support their customers with risk assessments, regulations should explicitly allow service providers to share standardized, replicable information about their products and services. This approach ensures customers get the necessary details without overwhelming providers with individualized requests, fostering a more streamlined and effective compliance process for everyone. Additionally, service providers should not be required to disclose trade secrets or intellectual property when complying with these obligations.	The Agency disagrees with this comment. The language in §§ 7050(h)(2) and 7153(a) is clear that a service provider, contractor, or relevant business must provide all necessary facts to businesses conducting risk assessments. It is unclear what the comment means by "standardized, replicable information." That information must have the necessary facts for recipient-businesses to conduct their risk assessments to be compliant with the regulations.
7051	255	Comment criticizes repeated changes to the Service Provider/Contractor Addendum template in § 7051, arguing that they create an unnecessary compliance burden.	This comment is not related to any modification to the text for the 15-day comment period.

ARTICLE 5. VERIFICATION OF REQUESTS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7060(a), (c)	585	Comment supports retaining verifications and the explicit permission to use third-party identity verification services. Comment also commends the rule requiring that verification processes scale in stringency with the sensitivity of the data.	The Agency agrees with this comment to the extent that it supports the Agency's regulations, and notes comment's support.
7060(e), (f)	586	Comment supports ban on consumer-paid verification fees and onerous procedures, such as requiring notarization as a condition of verification, except where reimbursement is required.	The Agency agrees with this comment to the extent that it supports the Agency's regulations, and notes comment's support.
Verification	587, 588, 589	Comment suggests newly requiring or clarifying existing multi-factor authentication and modern cryptographic verification requirements to require advanced identity-proofing technologies, such as cryptographic proofs or zero-knowledge proofs, to verify identity attributes. Comment suggests businesses should be required to adopt continuous, dynamic reauthorization methods for AI agents and non-human identities that verify all API interactions or automated requests in real-time. Comment advocates for businesses to take a proactive risk-based stance and to use dynamic risk scoring techniques to assess contextual factors to detect for fraud, such as geographic anomalies, behavioral patterns, and unusual request volumes. Verification stringency should escalate automatically when risks are detected.	This comment is not related to any modification to the text for the 15-day comment period. The Agency notes comment's suggestion and looks forward to continuing to work with stakeholders on future policy development.

ARTICLE 9. CYBERSECURITY AUDITS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7121	298	Comment appreciates flexibility for small businesses but finds the revisions introduce complexity and potential confusion. Comment recommends that the Agency revise § 7121 to	The Agency disagrees with this comment. The regulations are clear that only businesses that meet one of the thresholds in § 7120(b) must complete an annual cybersecurity audit. § 7121

		avoid potential conflict with § 7120, particularly for § 7121(a)(3), and clarify that the business must first meet the criteria of § 7120, i.e., for § 7121(a)(3), the business meets the threshold set forth in Civil Code § 1798.140(d)(1)(A) and the business' annual gross revenue for 2028 was less than fifty million dollars.	sets forth the timing requirements for such businesses' cybersecurity audits and audit reports.
7122(a)	299	Comment believes the regulation is too limited and should recognize a broader range of audit standards from other reputable organizations.	The Agency disagrees with this comment. The regulation already provides flexibility for businesses and their auditors to use "procedures and standards accepted in the profession of auditing." The examples listed are not exhaustive.
7122(a)(2)	243	Comment criticizes that the regulations prohibit auditors from making recommendations on the business's cybersecurity program. This would disincentivize auditors from making actionable observations without any apparent policy rationale.	The Agency disagrees with this comment, which appears to misinterpret the regulation. The regulation prohibits an auditor from participating in business activities that the auditor may assess in the current or subsequent audit. The regulations are clear that the prohibition against the auditor making recommendations regarding the business's cybersecurity program is "separate from articulating audit findings." The prohibition is consistent with the CCPA's direction to the Agency to establish a process to ensure the independence of cybersecurity audits.
7122(a)(3)	362	Comment supports the removal of the board reporting mandate, which allows oversight by executive management rather than the board, aligning better with operational governance structures.	The Agency agrees with this comment to the extent that it supports the Agency's regulations and notes comment's support.
7122(a)(3), 7122(f)	483	Comment criticizes the change in audit reporting lines: previously, auditors had to report to the board or governing body; now, they report to executive management, which may be less independent. Further, the requirement to submit the cybersecurity audit report to the board of directors or governing body has been watered down to require submission to the executive team with direct responsibility for the business's cybersecurity program. Requiring reporting to the board or the governing body that is incentivized to	The Agency agrees with this comment to the extent that it supports measures to ensure compliance and encourage independent, objective, and robust cybersecurity audits. Nevertheless, the Agency revised the regulations to remove board involvement requirements to simplify implementation for businesses at this time. For example, the Agency revised § 7122(a)(3) to remove requirements for board involvement and instead allow a member of the business's executive management team who does not have direct responsibility for

		ensure compliance and is not directly in charge of the auditing team would have encouraged more independent, objective, and robust cybersecurity audits. The Agency should reinstate the previous language for those provisions.	the cybersecurity program to fulfill those requirements. The regulations also no longer require that the cybersecurity audit report be reported to the board and instead allow it to be provided to a member of the business's executive management team who has direct responsibility for the cybersecurity program (*See* § 7122(f).) Although this is no longer required, businesses are not prohibited from involving their board or governing body in information related to the cybersecurity audit. Additionally, § 7122 provides clarity and guidance regarding auditor objectivity and independence and is consistent with practices in the current marketplace in other contexts. The regulations implement the requirements of the CCPA and balance providing privacy protections for consumers and flexibility for businesses.
7123(b)	31, 147	While the removal of language requiring cybersecurity audits to document and explain why cybersecurity program components are not necessary is welcome, comment reiterates its recommendation to strike the list of components now included in § 7123(c). Comment argues that the scope of the cybersecurity audit under § 7123(b) remains overly broad and insufficiently risk based, which risks diverting security resources toward compliance paperwork rather than substantive risk mitigation.	The Agency agrees with this comment to the extent that it supports the Agency's revisions to § 7123(b). The Agency disagrees with this comment's suggestion to remove the list of components in § 7123(c). The listed components are consistent with other cybersecurity frameworks and the CCPA's direction that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7123(b)(2)	484	Comment argues that the regulations diminish the scope of the cybersecurity audit. The new § 7123(b)(2) eliminates a prior requirement for businesses to explain why they exclude certain security components and how their alternatives provide equivalent protection. Silence regarding a component signals inadequacy of the business's practices. If the regulations allow for audits with such gaps, they should also include a presumption that when an incident occurs for which the omitted component could have served as a safeguard, the businesses practices as they related to the omitted component were not adequate, as they were not described in	The Agency disagrees with this comment. The regulations implement the requirements of the CCPA and balance providing privacy protections for consumers and flexibility for businesses. The comment's suggestion is not more effective or appropriate than the Agency's regulation. The Agency believes that no further modification is needed at this time. Separately, the CCPA already requires businesses to implement reasonable security procedures and practices. (*See* Civ. Code § 1798.100(e).)

		the audit.	
7123(c)	300, 354	Comment argues that § 7123(c)(1)(A) introduces uncertainty as it does not specify when multi-factor authentication is required, i.e., when accessing any information system as defined in § 7001(t). Comment recommends adding "for any individual accessing an information system." Comment argues that some of the most common cyber threats (e.g., business email compromise and phishing) exploit human vulnerabilities and are not explicitly addressed in the regulations' cybersecurity audit scope. Comment recommends amending § 7123(c)(8)(A) to explicitly include email security services in the audit criteria. Comment proposes that § 7123(c)(8)(A) be amended as follows: (A) Technologies, such as bot-detection, intrusion-detection, intrusion prevention, exfiltration detection, exfiltration prevention, and email fraud, phishing and other business email compromise prevention, which a business may use to detect unsuccessful login attempts, monitor the activity of authorized users, detect and prevent malicious email, protect a business's cloud applications, social media accounts and mobile devices, and detect and prevent unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information.	The Agency agrees with this comment to the extent that it supports proactive cybersecurity measures. The Agency disagrees with this comment's suggestion to further modify the regulations. The regulations are consistent with the CCPA's direction to the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) They do not require businesses to implement certain cybersecurity protections or practices. Rather, they provide clarity and guidance about how businesses must perform a thorough and independent cybersecurity audit. The regulation is reasonably clear based on the plain meaning of the words and the context in which they are used. The comment's suggestions are not more effective or appropriate than the Agency's regulation. The Agency believes that no further clarification is needed at this time. The regulations are clear that an audit may assess and document components of a cybersecurity program that are not set forth in §§ 7123 (b) or (c). (*See* § 7123(d).) Additionally, §§ 7123(c)(8) and (13) already address network monitoring and defenses and cybersecurity education and training more broadly.
7123(c)	485	Comment argues that the definition of "security incident" was changed from an occurrence that "actually or potentially" jeopardized the security of data, including unauthorized access, destruction, use, modification, or disclosure of personal information, to an occurrence that "actually or imminently" jeopardized the security of data. This change narrows the range of potential cybersecurity threats that the audit will assess in terms of how the business manages its responses. This would ultimately leave businesses less prepared to respond to incidents and jeopardize consumer	The Agency disagrees with this comment. The Agency modified the definition of "security incident" in response to public comments, to provide clarity to businesses and their auditors, and to simplify implementation for businesses at this time. The revised definition is consistent with how the National Institute of Standards and Technology ("NIST") defines "incident" in certain publications. (*See, e.g.*, NIST SP 800-53, Rev. 5.) In addition, the regulations clarify that nothing in § 7123 prohibits an audit from assessing and documenting components of a cybersecurity program that are not set forth

		privacy in the end. Custodians of consumer data can more effectively mitigate the severity of a potential security incident when the trigger to respond is potential jeopardy rather than imminent jeopardy—and the Agency's cybersecurity regulations should reflect that.	in §§ 7123 (b) or (c). (*See* § 7123(d).) Therefore, a business's cybersecurity audit could assess and document a business's responses to occurrences that potentially jeopardize the security of consumers' personal information.
7123(f)	32, 115, 149, 183, 226, 328, 363, 365, 397, 398, 462, 574	Comment argues that although § 7123 now suggests that businesses may rely on a prior cybersecurity audit conducted under another framework and cites audits that use the National Institute of Standards and Technology Cybersecurity Framework 2.0 as an example, it still could be read as requiring a detailed mapping to all regulatory requirements—even when the external audit was conducted using comprehensive and rigorous standards such as NIST CSF. The Agency should clarify that businesses may satisfy audit obligations by using such frameworks, provided they are implemented in good faith and reasonably address the regulation's core requirements, or provided that audits are conducted by qualified professionals using risk-based assessments. The Framework and other standards (e.g., International Organization for Standardization/International Electrotechnical Commission 27001 standard for information security management systems) are internationally recognized best practices. The Agency should avoid developing California-specific audit standards that diverge from proven national or international benchmarks and should consider reasonable conformance with such standards and frameworks, or conducting an audit or certification under leading global cybersecurity standards like ISO 27001 or SOC 2, as compliance with the requirements in Article 9. Comment proposes recognizing Payment Card Industry Data Security Standard (PCI DSS) reviews as satisfying the requirement. Comment proposes including NIST 800-53 and ISO 2701 as acceptable frameworks. Comment supports recognizing third-party audits (e.g., NIST CSF-based audits) as acceptable if they meet regulatory requirements. Comment argues that this	The Agency disagrees with this comment. § 7123(f) is clear that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the CCPA and regulatory requirements, either on its own or through supplementation; the Agency has also included an example. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. To the extent the comment suggests that the Agency should accept a business's use of a cybersecurity audit framework in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because a business's use of another framework does not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information. The regulations implement the CCPA's requirements, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements. The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to determine whether modifications to the regulations are necessary.

		approach would reduce burden and costs. Comment argues that relying on industry best practices will also avoid a situation in which the CPPA audit requirements become obsolete as technology advances. Comment argues that the Agency should recognize that equivalent audits for other jurisdictions undertaken by businesses should be deemed in compliance with the Agency. Comment suggests § 7123(f) should be as follows: A business may utilize a cybersecurity audit, assessment, or evaluation that it has prepared for another purpose, provided that it is reasonably similar in scope to this Article, either on its own or through supplementation. For example, a business may have engaged in an audit or certification that uses the National Institute of Standards and Technology Cybersecurity Framework 2.0, ISO 27001 certifications, SOC 2 audits, FedRAMP authorization, or similar audits and certifications. Such audits and certifications meet the requirements of this Article.	
7123(f)	117	Comment supports the change in the revised regulations that reference to the National Institute of Standards and Technology Cybersecurity Framework.	The Agency agrees with this comment and notes commenter's support.
7124	33	Comment argues that the revisions to § 7124 do not include language to permit businesses that engage in alternative cybersecurity audits, assessments, or valuations that meet the requirements of Article 9 to submit substitute documentation in lieu of certifications of completion. Comment maintains that the Agency should allow for substitute documentation, with recognition of their validity period, to reduce the regulatory burden on affected entities.	The Agency disagrees with this comment. "Substitute documentation" would not certify that the business had completed the cybersecurity audit required by the regulations.
CS Audits	1	Comment argues that cybersecurity audits are limited in driving cybersecurity outcomes. They are only reflective of a point in time and cannot reflect a real-time measure of the state of an organization's security posture. Comment cautions organizations against being overly reliant on the results.	The Agency agrees with the comment's warning against overreliance upon cybersecurity audits for determining cybersecurity posture and that audits provide a point-in-time assessment.

CS Audits	30	Comment supports the removal of the requirements for board members, governing body members, or highest-ranking executives to sign statements (§ 7122(i)) and written certifications (§ 7124(c)) regarding cybersecurity audits. Comment also supports the revision of the reporting requirement for auditors to include a member of an entity's executive management without direct responsibility for its cybersecurity program instead of a board member (§ 7122(a)(3)).	The Agency agrees with this comment and notes commenter's support.
CS Audits	34, 150	Comment argues that the Agency should consider incorporating a limited affirmative defense for companies that have completed a cybersecurity audit in good faith and implemented remediation plans for any identified gaps. The Agency should make clear that compliance with the cybersecurity audit regulations satisfies the CCPA's standard for reasonable care. Comment proposes that compliance with Article 9 be deemed an affirmative defense against claims under Civil Code § 1798.150(a)(1).	The Agency disagrees with this comment. The CCPA does not contain a provision that allows the Agency to determine if the business can use compliance with the regulations as an affirmative defense in litigation. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
CS Audits	116	Comment supports the changes in the regulations that requires audits be reported to a business's executive management team, rather than its board. Comment strongly support this change, because board members are not themselves subject matter experts and should be able to rely on the expertise of cybersecurity and other personnel for information about cybersecurity risks.	To the extent the comment supports the Agency's regulations, the Agency agrees with this comment and notes commenter's support.
CS Audits	118, 182, 224, 365, 430, 574	Comment asserts that the regulations do not address the concern that the cybersecurity audit threshold is too low and in conflict with the statutory text, inappropriately focus on the size of the business, and do not also consider the other statutorily-mandated factors when determining whether a cybersecurity audit is required. § 7120 is overbroad and inconsistent with the text of the statute, treating a business's processing as presenting "significant risk" simply because the business meets the minimum threshold for application of the	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to complete an annual cybersecurity audit, with the regulations establishing a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The CCPA requires the Agency to consider the size and complexity of the business, and the nature and scope of its processing activities, in determining

		statute. Commenter strongly supports the Agency's overarching commitment to enhancing cybersecurity but remains deeply concerned that the proliferation of state-specific cybersecurity mandates may lead to a fragmented regulatory landscape. Comment urges the Agency to adopt a risk-based framework rooted in widely accepted and operationalized industry standards. Comment requests that the Agency implement further changes to clarify that a business need not perform a cybersecurity audit unless the complexity, nature, and scope, in addition to size, of its processing activities each pose a significant risk to consumers' privacy and security. Comment recommends further amendments to align with existing California laws regulating the security of personal information, such as by revising the definition of "security incident" to narrow it or align with the existing definition of "security breach" in the California data breach notification law. Further, the Agency should revise the content required for cybersecurity audits to permit a risk-based approach that aligns with industry-recognized cybersecurity standards. Comment recommends that the Agency publish guidance including crosswalks between these California-specific requirements and leading frameworks, including the NIST CSF, ISO 27001, SOC 2, and programs like FedRAMP.	whether a business's processing of consumers' personal information presents significant risk to consumers' security. (*Id*.) The criteria in § 7120(b) are consistent with the CCPA and provide clarity for businesses in determining whether they are subject to the cybersecurity audit requirements. § 7120(b)(1)—deriving 50 percent or more of annual revenues from selling or sharing consumers' personal information—reflects the nature and scope of a business's processing activities and can be a proxy for the business's complexity. § 7120(b)(2)(a) and (b)—the revenue and personal-information processing thresholds—reflect the business's size and complexity and the nature and scope of its processing activities. Businesses whose processing of personal information meets either threshold in § 7120(b) present significant risk to consumers' security. The comment's suggestion that § 7120 treats being a regulated entity as presenting significant risk appears to reflect the comment's interpretation of the regulation, which is inconsistent with the regulations' language: § 7120(b) does not require all businesses subject to CCPA to complete a cybersecurity audit; it requires only businesses that meet specific one of the thresholds in § 7120(b) to complete a cybersecurity audit. In addition, the Agency has made efforts to limit the burden of the regulations while implementing the CCPA. Regarding the content of the cybersecurity audit, the regulations are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. Regarding the definition of "security incident," the Agency disagrees with the comment's suggestion to use California's breach-notification statute's definition of "security breach." It is not the same term, and California's breach-notification statute defines "personal information" more narrowly. The regulations are based upon CCPA's definition of "personal information"; the Agency cannot amend the CCPA or adopt

			regulations inconsistent with the CCPA. To the extent the comment suggests that alignment with other cybersecurity standards or use of a cybersecurity audit framework should be accepted in lieu of compliance with the regulations, the Agency disagrees, because a business's use of another framework does not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information. § 7123(f) is clear that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the requirements of Article 9, either on its own or through supplementation; the Agency also included an example. The regulations implement the CCPA's requirements, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements. To the extent the comment recommends that the Agency publish guidance, the comment is not on the proposed action, but the Agency notes the comment's suggestion and looks forward to working with stakeholders on future policy development.
CS Audits	119, 366	Comment asks the Agency to clarify that cybersecurity audit requirements apply only to data processed in a business capacity, not as a service provider. Comment recommends modifying § 7120(b) to state: A business's processing of consumers' personal information presents significant risk to consumers' security if any of the following is true for personal information it processes in its role as a business. Comment also suggests the Agency further revise § 7123(a) to state: The cybersecurity audit must assess how the business's cybersecurity program: protects personal information that it processes in its role as a business from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information.	The Agency disagrees with this comment. The regulations require a business that meets specific criteria to complete a cybersecurity audit. They are sufficiently clear that the cybersecurity audit would address the personal information processed by the business and the personal information that the business makes available to service providers, contractors, or third parties.

CS Audits	146	Comment acknowledges the changes to Article 9, including the removal of some of the overly prescriptive requirements such as mandatory Zero Trust Architecture and the addition of significantly improved governance provisions. However, the revised regulations continue to present operational challenges and lack sufficient alignment with industry standards, particularly in three critical areas: audit scope, audit cadence, and recognition of existing cybersecurity frameworks.	To the extent that the comment supports the Agency's regulations, the Agency agrees with this comment and notes commenter's support. To the extent the comment recommends additional revisions to the regulations, the Agency disagrees with this comment. The CCPA requires the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to "perform a cybersecurity audit on an annual basis," with the regulations defining the scope of the cybersecurity audit and establishing a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The Agency has made efforts to limit the burden of the regulations while implementing the law. The comment's suggestion that the cybersecurity audit cadence should not be annual would be inconsistent with the CCPA. Regarding the comment's suggestion that the regulations should further recognize existing cybersecurity frameworks, it is unclear what the comment is suggesting; however the regulations are consistent with other cybersecurity frameworks. § 7123(f) is clear that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the Article 9 requirements, either on its own or through supplementation; and includes an example.
CS Audits	148, 191, 218, 223, 225, 227, 328, 341, 396, 513	Comment requests that the Agency reconsider the mandatory annual audit requirement, which comment argues imposes significant burdens on regulated entities without a commensurate increase in data protection. Comment argues that the requirement imposes substantial and unnecessary financial and time burdens on service providers without providing demonstrable benefit to California businesses. Comment states that cybersecurity audits should be risk-based, consistent with industry standards and other cybersecurity frameworks, and that industry standards do not recommend extensive annual audits. Comment states that	The Agency disagrees with this comment. The CCPA requires the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to "perform a cybersecurity audit on an annual basis," with the regulations establishing a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The Agency has made efforts to limit the burden of the regulations while implementing the law. Not requiring businesses that meet one of the thresholds in § 7120(b) to complete an annual, thorough, and independent cybersecurity audit would be

		annual audits are not feasible for many businesses and are also inconsistent with global norms such as ISO 27001 and NIST frameworks. Comment suggests a more dynamic and flexible model, such as intervening audits and advocates for a three-year full audit cycle with annual limited-scope assessments in between. Comment recommends adding a definition of "Intervening cybersecurity audit" and permitting businesses to conduct a full cybersecurity audit every three years with annual "intervening" audits. Comment argues that businesses should have the flexibility to conduct a full cybersecurity audit every three years with annual audits or assessments only for materially changed or new conditions for the intervening years of the three-year cycle. Comment also recommends requiring certifications of compliance only every three years in connection with the full cybersecurity audit. Comment argues that the annual reporting requirement would potentially result in a waste of resources by focusing on formality over substance, failing to capture the dynamic nature of cybersecurity risks, which are evolving continuously.	inconsistent with the CCPA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Regarding certifications of completion, the Agency determined that the certification of completion requirements are relevant to the thoroughness and independence of the annual audit and therefore included the requirements.
CS Audits	220, 221, 223, 367	Comment advocates for clearly defined audit scopes, agreed upon via a pre-established audit plan, and cautions against open-ended provisions that create ambiguity and management difficulties. Comment argues that the regulations fail to allow service providers to use prepared cybersecurity audit materials as the first step in responding to an annual audit. Comment contends that individualized audit responses will divert critical cybersecurity resources toward document production and audit response management, unnecessarily shifting the focus of valuable security resources at service providers away from their day-to-day cybersecurity work and turn them into document production experts. The Agency should define a standardized set of cybersecurity information that service providers must supply to California businesses and amend the language to explicitly allow service	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to complete an annual cybersecurity audit, with the regulations establishing a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The regulations are consistent with the CCPA and provide clarity and guidance for businesses about how to perform an annual cybersecurity audit. They are meant to be robust and applicable to many factual situations and across industries. They are reasonably clear based on the plain meaning of the words and the context in which they are used. The Agency believes that no further clarification is needed at this time. Comment's recommendation regarding service providers supplying standardized cybersecurity

		providers to share standardized evidence of industry standard audits and certifications about their products and services.	information to California businesses is unclear. The regulations require service providers to cooperate with businesses for those businesses' cybersecurity audits. § 7050(h) is clear that a service provider must make available to business's auditor all relevant information that the business's auditor requests to complete the business's cybersecurity audit that is within the service provider's possession, custody, or control, and only with respect to personal information the service provider collected pursuant to its written contract with the business. The regulations implement the requirements of the CCPA and balance providing privacy protections for consumers and flexibility for businesses and their service providers. In addition, § 7123(f) is clear that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the Article 9 requirements, either on its own or through supplementation.
CS Audits	222	Comment argues that the rules lack an exception which allows a service provider to object to the disclosure of confidential, proprietary, or similar information in the audit. This could compromise the cybersecurity posture of businesses or disclose materials that are confidential or proprietary to them, and which provide them with a competitive advantage, including even trade secrets. If it is mandatory to disclose all cybersecurity methods, they may be less inclined to invest in competitive technologies if they must disclose their innovations without any carve-outs to every California business which asks in a mandatory annual audit.	The Agency disagrees with this comment. The requirements regarding service providers only apply to the personal information the service provider collected pursuant to its written contract with the business, and are clear that a service provider must make available to business's auditor all relevant information that the business's auditor requests to complete the business's cybersecurity audit that is within the service provider's possession, custody, or control. (*See* § 7050(h).) The regulations implement the requirements of the CCPA and balance providing privacy protections for consumers and flexibility for businesses and their service providers.
CS Audits	241, 242, 247, 249, 356, 357, 447, 574	Comment acknowledges the Agency's improvements on the modified regulations but criticizes the regulations as overly prescriptive and potentially contradictory to, or duplicative of, existing banking cybersecurity frameworks and federal standards imposed by the Office of the Comptroller of the Currency ("OCC"), the Federal Reserve, and the Federal Financial Institutions Examination Council ("FFIEC").	The Agency disagrees with this comment. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).)

		Comment argues the Agency lacks the statutory authority to adopt a prescriptive set of affirmative cybersecurity requirements. Comment urges the Agency to move away from prescriptive requirements that do not account for reasonable variations in approach among institutions of different sizes. Comment recommends removing or revising certain technical control requirements in §§ 7123(c)(E), (O), and (P). Comment urges the Agency to clarify and refine the scope of the cybersecurity audit provisions, and asks the Agency to permit businesses to conduct cyber audits under other commonly used risk frameworks, such as the NIST Framework for Improving Critical Infrastructure Cybersecurity and the Cyber Risk Institute Profile, or to permit businesses to fulfill the annual cybersecurity audit requirement by demonstrating adherence to existing, federally mandated cybersecurity audit processes. Comment argues that the Agency's changes to the reporting requirements for internal auditors highlight the problems with the Agency's overly prescriptive approach and that the revised language in § 7122(a)(3) raises significant concerns for banks subject to Federal Reserve guidance that may conflict with the proposal. Comment appreciates the removal of the previously proposed provisions mandating, as opposed to permitting, that the internal auditor report directly to the board of directors (former §7122(a)(3)), and other proposed board-related provisions (e.g., former §7122(f), §7124(e)), but asserts that the newly proposed text requiring that the highest-ranking auditor report to a member of executive management who does not have direct responsibility for the company's cybersecurity program (inclusive of evaluation of the auditor's performance and determination of compensation) is inconsistent with recommended best practices, which provides for direct or functional reporting to the audit committee of the board of directors or another board body. Comment cites 2024 IIA standards and a 2025 IIA survey	The regulations are consistent with this direction and authority, and they do not require businesses to implement certain cybersecurity protections or practices. Rather, they provide clarity and guidance about how businesses must perform a thorough and independent cybersecurity audit. The comment does not articulate a contradiction between the regulations and banking requirements or cybersecurity frameworks. In addition, the CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) Further, although this is no longer required, a business is not prohibited from having an internal auditor also report to the business's board or audit committee, and it is not uncommon for one or more members of a business's executive management team to also be a member of the business's board. The comment's suggestions are not more effective or appropriate than the Agency's regulation. § 7123(f) is clear that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the Article 9 requirements, either on its own or through supplementation; the Agency has also included an example. To the extent the comment suggests that the Agency should accept a business's use of a cybersecurity audit framework in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because a business's use of another framework does not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information. The regulations are necessary to implement the CCPA's requirements, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements.

		showing that over 90% of companies maintain a functional reporting line between internal audit and the board. Comment recommends modifying § 7122 to permit reporting either to the board (preferred best practice) or to a non-cybersecurity executive. Comment recommends providing companies with more flexibility, including to choose structures that align with their governance models and ensure auditor independence. Comment suggests proposed text as follows: If a business uses an internal auditor, to maintain the auditor's independence, the highest-ranking auditor must report directly either to the board of directors or a committee of the board of directors (such as the audit committee) or a member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program. As used herein, direct reporting shall include conducting the highest-ranking auditor's performance evaluation, if any, and determining such auditor's compensation.	
CS Audits	248, 355, 431, 574	Comment argues that §§ 7123(e)(3) and 7121(a)–(d) do not address commenters' concerns that that the cybersecurity audit requirements will inadvertently undermine businesses' security by requiring them to disclose information that could enable malicious actors to bypass security measures. Comment believes that the revised rules essentially require that auditors produce a roadmap for defeating a business's security measures, jeopardizing the security of consumers' personal information. Comment suggests that companies must not be forced to reveal proprietary methods or trade secrets as part of their cybersecurity audit reporting. Comment requests that the cybersecurity audit requirements be modified to limit the information that must be included in a cybersecurity audit report, permit businesses to exclude information that they deem to be sensitive, and clarify that businesses are not required to disclose trade secrets (as defined in Civil Code § 3426.1(d)) in the cybersecurity audit	The Agency disagrees with this comment. The CCPA directs the Agency to establish a process to ensure that audits are thorough and to define the scope of the audit. (Civ. Code § 1798.185(a)(14)(A).) Requiring the cybersecurity audit to include information about the business's cybersecurity posture, including the gaps and weaknesses in its cybersecurity program, is part of ensuring that the audit is thorough and is consistent with the CCPA's direction to the Agency. The comment's interpretation of the regulations appears to be inconsistent with the regulations' language, which require a business to submit a certification of completion to the Agency, not its cybersecurity audit report. (*See* § 7124.) Additionally, providing disclosures to the Agency does not equate to it being disclosed; whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the Public Records Act ("PRA") applies. The Agency is also required to comply with

		reports as follows: § 7123(g) In creating the cybersecurity audit and report required by this § 7123, neither a business nor a service provider is required to disclose information relating to Trade Secrets, as defined in Civil Code § 3426.1(d). Comment argues that the draft rules do not provide adequate protections for the confidentiality of audit materials. Agency should confirm that it will take precautions to protect audits received from businesses against breaches or inappropriate disclosure, including by clarifying that audits will be treated as confidential and exempt from disclosure under public records laws. To protect businesses and consumers, all personal information and confidential business information should be redacted from the audits 30 days after they are received by the Agency.	the Information Practices Act of 1977. (*See* Civ. Code §§ 1798–1798.78.)
CS Audits	292	Comment argues that the Agency should encourage the inclusion of privacy assessments in standard audits, such as SOC 2 reports. A principle-based approach (e.g., the Privacy Trust Principle) would support consistency and accountability.	The Agency agrees with this comment to the extent that it supports businesses being able to utilize cybersecurity assessment work they have already done. The Agency disagrees with this comment's recommendation to further revise the regulations. § 7123(f) is clear that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the Article 9 requirements, either on its own or through supplementation disagrees with this comment. The comment's suggestions are not more effective or appropriate than the Agency's regulation.
CS Audits	358	Comment argues that the cybersecurity audit requirement under §§ 7120–7123 is too burdensome for small and medium size enterprises with limited budgets and IT resources. Comment urges the Agency to adopt a tiered audit framework similar to Colorado's Privacy Act Rule 6.09, where applicability thresholds are based on data risk level and business size or revenue. This would maintain accountability without imposing disproportionate burdens.	The Agency disagrees with this comment. The majority of the costs of the regulations fall on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million. Additionally, the CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform an annual cybersecurity audit, and establishing a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The CCPA also requires the

			Agency to consider the size and complexity of the business, and the nature and scope of its processing activities, in determining whether a business's processing of consumers' personal information presents significant risk to consumers' security. (*Id*.) The criteria in § 7120(b) already take business size and revenue into account. Businesses whose processing of personal information meets one of the thresholds in § 7120(b) present significant risk to consumers' security. Further, the Agency has made efforts to limit the burden of the regulations while implementing the CCPA. It is unclear what the commenter is suggesting regarding Colorado Privacy Act Rule 6.09, because that rule does not require a cybersecurity audit and does not include a tiered audit framework. Although the Agency strives for alignment with other privacy and security laws when appropriate, it must comply with California law and use its discretion to adopt requirements appropriate to California.
CS Audits	395	Comment states that the cybersecurity audit requirements are excessive and burdensome and diverts resources from protecting personal information and enterprise.	The Agency disagrees with this comment. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The regulations are consistent with this direction, and the Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations balance protections for consumers' security and simplifying implementation for businesses at this time.
CS Audits	486	Comment states that the May 2025 draft delays compliance deadlines for cybersecurity audits by up to five years, depending on business size. Comment argues this delay is unjustified and increases consumer risk, especially since many businesses already perform similar audits.	The Agency agrees with this comment to the extent that it supports decreasing risks to consumers' privacy. Nevertheless, the Agency modified § 7121 to phase in implementation by annual gross revenue over a three-year period to simplify implementation for businesses by reducing their costs to comply with the regulations, while still protecting consumers. The regulations appropriately balance protections for

			consumers' security and simplifying implementation for businesses.
CS Audits	590	Comment supports retention of multi-factor authentication, encryption of personal information at rest and in transit, rigorous account management and access controls, and mandatory security training and awareness.	The Agency agrees with this comment to the extent that it supports the Agency's regulations and notes comment's support.
CS Audits	584, 590, 591, 592	Comment supports preservation of multi-factor authentication, third-party identity verification, encryption of personal information at rest and in transit, rigorous account management and access controls, and mandatory security training and awareness. Comment expresses concern with the removal of zero trust architecture from the list of security program components and recommends requiring businesses to continuously verify user access and network integrity. This also includes measures such as dynamic risk-based authentication (re-authenticating or challenging users when anomalies are detected or context changes) and attribute-based access control (evaluating the user's role, device security, location, and other attributes before granting access). Utilizing hardened virtual appliances with tiered component positioning, assume-breach architecture, and internal service isolation should be treated as meeting zero-trust standards. Comment suggests clarifying that "restricting access to what is necessary" includes ongoing monitoring of access sessions and automatic blocking of unauthorized lateral movement.	The Agency agrees with this comment to the extent that it supports proactive cybersecurity measures and the Agency's regulations. Nevertheless, the Agency deleted zero-trust architecture to simplify implementation at this time. The regulations are clear that an audit may assess and document components of a cybersecurity program that are not set forth in §§ 7123 (b) or (c). (*See* § 7123(d).) Additionally, §§ 7123(c)(1), (3), and (8) already address authentication, access controls, and network monitoring and defenses more broadly. Therefore, a business's cybersecurity audit could assess and document a business's use of zero trust architecture, dynamic risk-based authentication, ongoing monitoring of access, automatic blocking of unauthorized lateral movement, attribute-based access controls, or hardened virtual appliances. The comment's suggestions are not more effective or appropriate than the Agency's regulation. Further, the regulations are consistent with the CCPA's direction to the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. They do not require businesses to implement certain cybersecurity protections or practices. Rather, the regulations provide clarity and guidance about how businesses must perform a thorough and independent cybersecurity audit.
CS Audits	593, 594, 595, 596, 597, 598	Comment recommends businesses be required to use strong, modern encryption algorithms and to assess their cryptographic algorithms for emerging threats, such as quantum computing. Businesses should have a migration plan	The Agency agrees with this comment to the extent that it supports proactive cybersecurity measures and the Agency's regulations. However, the CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to

		for quantum-resistant encryption. Comment recommends modifications that would allow file and disk double encryption to satisfy enhanced encryption standards. Businesses using TLS 1.3, AES-256 encryption, and FIPS 140-3 validated encryption standards should meet advanced encryption-in-transit requirements. Security platforms with integrated encryption approaches provide superior consumer protection to multiple separate and potentially less secure encryption implementations. Comment recommends requiring network monitoring intrusion detection/prevention systems to include real-time, continuous monitoring. Comment recommends continuous monitoring to complement annual audits. Comment recommends that Article 9 mandate governance of non-human identities, such as AI agents, API keys, automated bots, and service accounts. These identities should undergo continuous re-validation and context-aware risk assessments. Each identity should have an identified owner, minimal privileges, and be rotated or revoked when no longer needed (similar to employees). Access should be purpose-limited, restricted, and monitored as with human users. Comment recommends extending compliance oversight of service providers, contracts, and third parties to include security assessments of vendors, particularly those handling personal information or providing critical technologies, such as AI systems. Businesses often rely on third-party software or AI models to process consumer data. The audit rule should encourage companies to inventory critical vendors and evaluate vendors' security practices and reliability.	ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The regulations are consistent with this direction and do not require businesses to implement certain cybersecurity protections or practices. Rather, they provide clarity and guidance about how businesses must perform a thorough and independent cybersecurity audit. In addition, §§ 7123(c)(2), (3), (8), and (15) already address encryption; account management and access controls, including restricting accounts' and applications' access and privileges; network monitoring and defenses; and oversight of service providers, contractors, and third parties more broadly. Moreover, the CCPA already requires businesses to contractually require their service providers and contractors to provide the same level of privacy protection as is required of businesses by the CCPA and existing regulations, and existing regulations address the role of the business's due diligence with respect to their service providers, contractors, and third parties. (*See, e.g.* Civ. Code §§ 1798.100(e), (d)(2); §§ 7050-7053.) Further, the regulations are clear that an audit may assess and document components of a cybersecurity program that are not set forth in §§ 7123 (b) or (c). (*See* § 7123(d).) Therefore, a business's cybersecurity audit could assess and document a business's use of integrated encryption or real-time continuous monitoring. The comment's suggestions are not more effective or appropriate than the Agency's regulation.
CS Audits, 7050	219	Comment argues that the regulations fail to define the scope of the audit or to allow any objections, other than, "relevant information."	The Agency disagrees with this comment. The regulations are consistent with the CCPA and provide clarity and guidance for businesses about how to perform an annual cybersecurity audit. They are meant to be robust and applicable to many factual situations and across industries. They are reasonably clear based on the plain meaning of the words and the context

			in which they are used. For example, each cybersecurity audit must meet the requirements set forth in Article 9, including § 7123. The regulations are also reasonably clear that service providers and contractors must, with respect to the personal information that they collected pursuant to their written contract with the business, cooperate with the business in the business's completion of its cybersecurity audit. (*See* § 7050(h).) The Agency believes that no further clarification is needed at this time.

ARTICLE 10. RISK ASSESSMENTS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7150(b)	35, 401	Comment supports removing "significant decisions" and "extensive profiling" from §§ 7150(b)(3)(A)-(B), arguing that ADMT should not be subject to risk assessments under CCPA. Comment states that the definition of "significant risk" goes beyond the statutory text.	The Agency disagrees with this comment. The comment appears to reflect the comment's interpretation of the CCPA, which is inconsistent with the language, structure, and intent of the CCPA. Specifically, the CCPA directs the Agency to issue regulations requiring risk assessments for processing that presents significant risk to consumers' privacy. The use of ADMT for significant decisions presents significant risk to consumers' privacy, such as undermining control of personal information and unlawful discrimination. Businesses must still conduct a risk assessment for the use of ADMT for a significant decision, as set forth in § 7150(b)(3). With respect to extensive profiling, the Agency removed this term from the regulations to simplify implementation at this time. However, businesses must still conduct a risk assessment for certain automated processing in the workplace, in educational settings, or based on sensitive locations. This processing also presents significant risk to consumers' privacy, such as less consumer control over personal information, insufficient transparency, excessive surveillance, and unlawful discrimination and stigmatization.

7150(b)	131, 313, 327, 452, 521, 543, 551	Comment recommends revisions to § 7150(b)(3) to use a "reasonably foreseeable risk" standard with specific risk categories. Comment also seeks removal of §§ 7150(b)(4) and (5). Comment recommends removing § 7150(b)(5) because this information can be publicly available and the CPRA already covers sensitive location data regardless of the location's sensitivity. This threshold does not grant additional data protection and may deny local businesses the opportunity to offer their customers certain benefits. Also, the overbreadth here would capture low-risk activities such as providing discounts. Consumers do not have a reasonable expectation of privacy in a public place, and the CPRA already regulates the use of data collected from geo-trackers and precise geolocation. There also remains concerns about statutory authority. Alternatively, comment supports narrowing the rule to "sensitive locations" but argues that risk assessments should only be triggered when a consumer is identified at such locations and the data is used for profiling. Comment recommends changes as follows: § 7150(b)(5): "Using automated processing to infer or extrapolate a consumer's intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior, or movements, based upon that consumer's known or inferred presence in a sensitive location. 'Infer or extrapolate' does not include a business using a consumer's personal information to make inferences that do not relate to the sensitivity of the location, such as to provide goods or services requested by the consumer, to deliver goods to, or provide directions to or transportation for, that consumer at a sensitive location. For example, a consumer's presence in a sensitive location is not 'known or inferred' by a business if: (A) The business infers an interest in pets based on a visit to a pet store that happened to be next to an urgent care facility; or (B) The business provides a	The Agency disagrees with this comment. With respect to § 7150(b)(3), this threshold is clear. Comment's suggestion is no clearer and no more effective than the regulation. With respect to §§ 7150(b)(4)–(b)(5), the Agency disagrees with removing these thresholds. With respect to authority, the thresholds are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment. (*See* Civ. Code § 1798.145(a)(14)(B).) This includes automated processing that develops inferences or extrapolations about consumers in the workplace, in educational settings, and in sensitive locations, because this processing presents significant risk to consumers' privacy, such as undermining their control over their personal information. The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) §§ 7150(b)(4)–(b)(5) are not overly broad and are necessary to clarify the types of automated processing that present significant risk to consumers' privacy. In addition, § 7150(b)(5) addresses personal information, not publicly available information. Sensitive locations are not de facto "publicly available information" under the CCPA. Further, this threshold addresses certain automated processing based on a consumer's presence in these sensitive locations. This threshold is a distinct from the "processing sensitive personal information" threshold. In addition, to the extent these thresholds overlap for a single processing activity, it does not pose undue burden on businesses because they are only required to conduct a single risk assessment. (*See* § 7156(a).) The comment also does not explain how businesses would be denied the opportunity to offer customers benefits after conducting a risk assessment. The Agency does not believe this is the case. Rather, a risk assessment requires businesses to

		service regardless of location sensitivity, such as to deliver goods, provide directions or transportation to a sensitive location, and does not infer sensitive personal information based on that consumer's presence at a sensitive location. § 7001(aaa): "'Sensitive location' means any of the following physical places: healthcare facilities including hospitals, doctors' offices, urgent care facilities, and community health clinics; pharmacies; domestic violence shelters; food pantries; housing/emergency shelters; union offices; and places of worship." Comment proposes new § 7150(b)(7) as follows: "A risk assessment completed under another law that is substantially similar to the assessment required under this Article will satisfy the requirements of this Article."	identify relevant privacy risks and safeguards before initiating the processing, which supports both consumer privacy and business operations. The comment's suggested language is not necessary because the regulation is reasonably clear and does not encompass low-risk activities. In addition, the comment's proposed addition of § 7150(b)(7) is not necessary and is less clear than the regulation in § 7156(b). In § 7156(b), the Agency addresses how businesses can use risk assessments completed for another purpose to comply with § 7152.
7150(b)	238	Comment recommends that the Agency require risk assessments only for selling, sharing (for cross-context behavioral advertising), processing sensitive information (subject to exemptions for routine processing activities, such as those specified under § 7027(m)), and "significant decisions." Thus, the Agency should delete the currently proposed §§ 7150(b)(4), (b)(5), and (b)(6) and any corresponding examples in § 7150(c). This will make the regulations consistent with other jurisdiction and avoid forcing businesses to churn out paperwork. The Agency should also provide exemptions for activities subject to examination or supervision by a federal prudential regulator, if not a broader exemption for banking organizations.	The Agency disagrees with this comment. The comment's recommended thresholds would be less effective than the regulation and would exclude processing that presents significant risk to consumers' privacy, such as certain automated processing and training uses of consumers' personal information. The comment's recommendation would also make the regulations less consistent with approaches taken in other jurisdictions, such as the EU and Colorado. Further, additional regulatory exceptions are not necessary. Moreover, exempting financial institutions would be inconsistent with the CCPA, which instead includes a data-level exemption for information subject to the GLBA and implementing regulations; it applies to "businesses" and does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), 1798.145(e).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, the regulations do not force businesses to churn out paperwork, but rather require businesses to meaningfully identify benefits, risks, and safeguards.
7150(b)	400	Comment recommends deferring or minimizing prescriptive risk assessment language given active legislation in California around the topic and to avoid confusion or inconsistency.	The Agency disagrees with this comment. The Agency is required to issue regulations requiring risk assessments. (*See* Civ. Code § 1798.185(a)(14)(B).) They also do not conflict with

			California law and are clear about the scope of businesses' obligations. Further, delaying the regulations would be less effective at protecting consumer privacy.
7150(b)	368	Comment supports the revisions that narrow the ADMT and AI training triggers for risk assessments. The training process itself does not pose the same direct consumer risks associated with the processing of personal information for decision-making.	The Agency agrees with this comment to the extent that it supports the Agency's regulations and notes the comment's support. The Agency disagrees with the comment to the extent that it suggests that training uses of personal information do not pose significant risk to consumers' privacy. Training uses of consumers' personal information do pose significant risk to consumers' privacy, such as data leakage that can reidentify consumers whose personal information was used to train the model and a lack of transparency and consumer control over the use of their personal information for training.
7150(b)	405	Comment requests clarification that California's approach aligns with risk-based proposals in Colorado for ADMTs that are put into actual use.	The Agency disagrees with this comment. The Agency strives for harmonization with other jurisdictions as appropriate but must implement the CCPA's requirements and further the intent and purposes of the statute. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment. Training uses of consumers' personal information pose significant risk to consumers' privacy, such as data leakage that can reidentify consumers whose personal information was used to train the model and a lack of transparency and consumer control over the use of their personal information for training. The regulations are consistent with the approach taken in Colorado as applicable, while furthering the intent and purposes of the CCPA and providing clarity to businesses regarding their obligations.
7150(b)	467	Comment criticizes the removal of first-party behavioral advertising from the list. Profiling for behavioral advertising poses consumer privacy and equity risks and should therefore trigger the risk assessment requirement.	The Agency notes the comment's concerns. The Agency revised the regulations to simplify implementation for businesses at this time. The regulations continue to balance providing privacy protections for consumers with flexibility for businesses to come into compliance.

7150(b), 7152	179	Comment believes that the risk assessment requirements need substantial further revisions to align with the statutory text and voter intent regarding the processing thresholds and contents for such assessments. Specifically, the Agency must delete low-risk processing activities from the activities that require risk assessments, which do not satisfy the statute's clear direction to require risk assessments for processing activities that present "significant" privacy risk. For example, the use of ADMT for allocation or assignment of work and compensation should be deleted, as should the threshold based on presence in a public location. The thresholds should be limited to sale/sharing, processing sensitive personal information unless subject to § 7027(m), and the use of ADMT to reach a significant decision that imposes significant risk to consumer privacy. The Agency should also remove requirements unrelated to privacy and permit businesses flexibility to address criteria relevant for the processing activity. Notably, the statute contemplates privacy risk assessments, and thus, discussions of "economic harms," "physical harms," and other topics with no relation to privacy should be removed. Further, the current list of inflexible topics a business "must" consider results in a burdensome paperwork exercise that contravenes the explicit statutory direction to engage in a risk-based balancing exercise. The Agency provides no evidence that addressing each of these topics is necessary to prevent consumer harm. The Agency should therefore prioritize a flexible set of criteria that the business can tailor to the circumstances of a particular processing activity and that is interoperable across U.S. privacy laws, rather than an inflexible check-the-box exercise that is unlikely to keep paces with changes in technologies and divert business resources towards a paperwork exercise without consumer benefit.	The Agency disagrees with this comment. Each of the processing activities in § 7150(b) present significant risk to consumers' privacy. For example, the use of ADMT to make significant a decision about a consumer, including to allocate or assign work, can lead to unlawful discrimination based on protected characteristics, lack of consumer control over their personal information, and economic harm. Similarly, automated inferences or extrapolations about a consumer based on their presence in sensitive locations present significant risk to consumers' privacy. For example, consumers may not expect their devices to be tracked in these locations to develop inferences or extrapolations about them. The comment's recommended thresholds would be less effective than the regulation at protecting consumer privacy. With respect to § 7152, privacy risks include economic and physical harms to consumers. This is consistent with both common-sense understandings of privacy harms and with other jurisdictions' approaches to privacy, such as the EU and Colorado. The regulations also provide examples as guidance of how processing personal information can result in different negative privacy impacts. In addition, the Agency revised the regulation to state that this is a non-exhaustive list of harms that businesses may consider when identifying privacy risks to consumers, which provides both clarity and flexibility for businesses. The comment does not explain why the topics identified in § 7152 would be unduly burdensome for businesses to identify, and the Agency disagrees with this point. The requirements in § 7152 are necessary to adequately identify the benefits and potential risks of a given processing activity. The regulations are also adaptable to a variety of contexts and enable businesses to leverage existing compliance processes to comply with their requirements.

7150(b), 7152	215	Comment recommends limiting risk assessment requirements to ADMTs actually used in consequential decisions, rather than applying to training activities or overly broad definitions of "significant risk," which go beyond the statutory mandate and intent. Moreover, references to profiling based on "sensitive locations" must distinguish between routine uses (e.g., geofencing for store locations) and invasive surveillance. Granular reporting mandates, including disclosing ADMT "logic," threaten trade secrets and impose excessive burdens without improving consumer protection. Aligning with interoperable, risk-based models would support stronger outcomes.	The Agency disagrees with this comment. The risk assessment thresholds are within the Agency's authority to require risk assessments for processing that presents significant risk to consumers' privacy and further the intent and purposes of the CCPA. § 7150(b) presents six thresholds, including the training threshold, that clarify which processing constitutes significant risk. These are not overly broad; they focus on a limited set of processing activities. The threshold regarding sensitive locations is focused on specific types of inferences and extrapolations about a consumer and is not overly broad. With respect to risk assessment requirements, the logic requirement is not burdensome. § 7152(a)(3)(G)(i) provides clear requirements regarding identifying the logic of the ADMT and how it works, including its assumptions and limitations, which is necessary to identify privacy risks to consumers when using that ADMT to make a significant decision about them. Businesses can also leverage existing compliance processes to comply with the requirements of § 7152, which promotes interoperability. Further, with respect to trade secrets, the CCPA does not require businesses to divulge trade secrets in risk assessments. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7150(b), 7156(b)	134	Comment recommends allowing a risk assessment that satisfies another jurisdiction's requirements to be substituted for the list of requirements in this section, even if they do not meet every requirement listed in § 7152(a)(3). Additionally, other state privacy laws require risk assessments only when "sensitive data" is processed or for profiling that results in specific consumer harms.	The Agency disagrees with this comment. § 7156(b) is clear that businesses can leverage existing compliance processes while meeting the CCPA's requirements for a risk assessment. The comment's recommendation would be less effective at protecting consumer privacy, because it would not ensure that businesses conduct thorough and comprehensive risk assessments as set forth in these regulations. In addition, the regulations are consistent with other jurisdictions while furthering the intent and purposes of the CCPA and providing clarity to businesses regarding the scope of their obligations. Each of the thresholds in § 7150(b) presents significant risk to consumers' privacy and therefore would require a risk assessment. Narrowing the thresholds would be less effective at

			protecting consumer privacy and would be inconsistent with other privacy frameworks, such as the GDPR and the Colorado Privacy Act.
7150(b)(1)	95, 126	Comment argues that "significant risk" should be limited to the selling or sharing of "sensitive" personal information rather than all personal information. Without such a limitation, the use of tracking technologies such as cookies could be considered a significant risk to consumers for which businesses would need to conduct a risk assessment. This is overbroad and unnecessary.	The Agency disagrees with this comment. Selling or sharing personal information presents significant risk to consumers' privacy, such as impairing consumers' control of their personal information, imposing economic costs on consumers, and creating opportunities for criminal activity. In addition, this threshold is consistent with approaches taken under other jurisdictions, such as Colorado. To the extent a tracking technology involves the selling or sharing personal information, it would require a risk assessment. This is not over broad or unnecessary, but rather ensures that businesses identify and mitigate relevant privacy risks for processing that presents significant risk to consumers' privacy.
7150(b)(2)	96, 126, 370	Comment states that the exemption around processing sensitive personal information in employment-related contexts is likely to create confusion due to the current approach of listing specific examples, which are too narrow and may lead to inconsistent interpretations among companies. Comment recommends adding a catch-all for all employment-related purposes or language stating that such purposes "include, but are not limited to" the enumerated types of purposes. Limiting the list of employment-related purposes is too narrow and may exclude other legitimate employment-related purposes. Comment recommends the following language: "A business that processes the sensitive personal information of its employees or independent contractors solely and specifically for employment-related purposes is not required to conduct a risk assessment for the processing of sensitive personal information for these purposes. Any other processing of consumers' sensitive personal information is subject to the risk-assessment requirements set forth in this Article."	The Agency disagrees with this comment. The comment's recommendation is not more effective or appropriate than the Agency's regulations, and it would be less clear. It is unclear what an "employment-related purpose" is; the exception would make compliance more difficult for businesses and be less effective at protecting consumer privacy.

7150(b)(2)	237	Comment argues that the processing of sensitive information should not trigger a risk assessment when the sensitive personal data is being processed only for purposes specified in § 7027(m) of the Agency's existing rules.	The Agency disagrees with this comment. Processing sensitive personal information for the purposes identified in § 7027(m) can still present significant risk to consumers' privacy. For example, even if a business is not using a social security number to infer characteristics about a consumer, processing this information can still pose significant risk to consumers' privacy, such as the risk of unauthorized access if the information is not stored securely.
7150(b)(3)	556	Comment argues that § 7150(a)(1) extends application to all uses of ADMTs for decisions regarding provision of, denial of, or access to employment and employment compensation. Comment suggests narrowing employment and contractor decisions.	There is no § 7150(a)(1). The comment also appears to refer to the proposed text published on November 22, 2024, not to the modified text of proposed regulations published on May 9, 2025. The modified text of proposed regulations published on May 9, 2025, reflects that the Agency removed the term "access to" from the definition of significant decision. To the extent comment is requesting limiting the ADMT threshold in § 7150(b)(3), the Agency disagrees with this comment. The use of ADMT for employment or independent contracting opportunities or compensation presents significant risk to consumers' privacy, such as undermining their control over their personal information and discrimination.
7150(b)(4)	520	Comment suggests striking § 7150(b)(4) entirely.	The Agency disagrees with this comment. The Agency determined that this type of automated processing presents significant risk to consumers' privacy, such as less consumer control over personal information, insufficient transparency, excessive surveillance, and unlawful discrimination; the regulations therefore require a risk assessment.
7150(b)(4), (b)(5)	309	Comment commends the modified draft made significant improvements to establish rules that are more risk-based by focusing on using ADMT for a significant decision concerning a consumer. However, there are some inconsistencies in the regulations that should be addressed to ensure a more harmonized, risk-based approach. §§ 7150(b)(4) and 7150(b)(5) are overly broad because they reference "automated processing" instead of ADMT. Comment notes	The Agency disagrees with this comment. §§ 7150(b)(4)-(5) are not overly broad, and the term "automated processing" is reasonably clear. In addition, these thresholds do not introduce uncertainty or lack of clarity to the regulations. They are clear that if a business is engaging in automated processing as set forth in a given threshold, it must conduct a risk assessment. These are separate from the ADMT threshold in § 7150(b)(3), which specifically addresses the use of ADMT to make a

		that "automated processing" is not a defined term within the proposal. Inclusion of "automated processing" together with the other references to "ADMT"—a term that has been carefully contemplated and defined—will introduce uncertainty and risk an overbroad interpretation of these sections. It is not clear that §§ 7150(b)(4) and 7150(b)(5) are focused on ADMT used for significant decisions, which is inconsistent with the other rules. § 7150(b)(4)'s reference to "systematic observation" raises First Amendment concerns to the extent that it sweeps in technology based on publicly available or publicly observable information. Comment recommends that § 7150(b)(4) should be struck entirely. § 7150(b)(5) should be amended as follows: "Using ADMT to make a significant decision concerning a consumer based upon that consumer's presence in a sensitive location."	significant decision. With respect to the definition of "systematic observation," the Agency disagrees that this definition raises First Amendment concerns or encompasses publicly available information. Further, the comment's recommendations would make the regulations less effective at protecting consumer privacy because it would exclude from the risk assessment requirements certain automated processing in the workplace, in educational settings, and based on sensitive locations.
7150(b)(5)	36	Comment states that the modified rules add the concept of "sensitive location," and § 7150 adds a requirement to complete a risk assessment before "profiling a consumer based upon their presence in a sensitive location." Comment requests that the Agency specify that this list is exhaustive.	The Agency disagrees with this comment to the extent that it argues that the regulation is not clear. The definition of "sensitive location" is clear and specifically lists physical places that are sensitive locations. It is not necessary to specify that the list is non-exhaustive because the regulation already clearly states that "sensitive locations" are any of the places listed in the definition.
7150(b)(5)	82, 402, 453	Comment suggests that § 7150(b)(5) should be reassessed. The provision still creates operational uncertainty and compliance costs for businesses whose data practices may not pose real privacy risks, such as providing discounts for prescriptions at specific pharmacies based on a consumer's prior use or college merchandise based on a student's residence at college. This would require risk assessments based on nonsensitive, low-risk, and publicly available information. Thus, comment recommends removal of this provision to enhance clarity and reduce administrative burdens on businesses. Alternatively, comment recommends that for profiling in a sensitive location under § 7150(b)(5),	The Agency disagrees with this comment. § 7150(b) applies to risk assessments and does not trigger ADMT opt-outs, which are addressed in Article 11. Additionally, the threshold is not overly broad but rather addresses a narrow list of sensitive locations that present heightened privacy risks for consumers. For example, consumers may not expect their devices to be tracked in these locations to develop inferences or extrapolations about them. The regulation also does not create operational uncertainty or pose undue burden on businesses. Rather, a risk assessment requires businesses to identify relevant privacy risks and safeguards before initiating the

		the rule should clarify that only sensitive and consequential uses of location profiling are regulated. This prevents basic tools like geofencing or location-tagging from needing to comply with ADMT opt-outs and risk assessments. To the extent the definition of "sensitive location" does not change, comment recommends striking § 7150(b)(5).	processing, which supports both consumer privacy and business operations.
7150(b)(5)	60	Comment expresses concern that the definition of "sensitive location" is overly broad and could have far-reaching unintended consequences as it includes benign locations such as educational institutions and legal services offices, which could complicate standard business marketing operations and frustrate consumer expectations. In addition, the requirement risks chilling lawful commercial speech and limiting advertising on important topics, including advertising to doctors and healthcare workers. As drafted, the "sensitive location" definition and related risk assessment requirements would unreasonably burden free speech through advertising in or near any location the Agency has deemed to be "sensitive."	The Agency disagrees with this comment. The definition of "sensitive location" is not overly broad. It provides a narrow list of places that present heightened privacy risks for consumers. For example, visits to legal services offices can reveal a consumer's interest in sensitive topics, such as receiving advice on immigration or criminal law. Public comments have recommended inclusion of places such as educational institutions because these places present discrete privacy issues or could reveal sensitive information about a consumer. It is unclear how conducting a risk assessment would complicate marketing operations, frustrate consumer operations, or limit advertising. Rather, a risk assessment requires businesses to identify relevant privacy risks and safeguards before initiating the processing, which supports both consumer privacy and business operations. Further, the Agency disagrees that this regulation would unreasonably burden free speech.
7150(b)(6)	562	Comment argues the threshold in § 7150(a)(3) regarding AI/ADMT training should be limited in scope.	The regulations do not include § 7150(a)(3). To the extent comment is requesting limiting the training threshold in § 7150(b)(6), the Agency disagrees with this comment. The training threshold is necessary to address processing that presents significant risk to consumers' privacy. After receiving initial comments, the Agency revised the regulation to add an intent-based standard and narrow the training uses covered. This further simplifies implementation for businesses at this time.
7150(b)(6)	75, 180	Comment believes that the regulations improperly introduce a separate risk assessment requirement for "physical or biological identification or profiling," which substantially	The Agency disagrees with this comment. The training threshold is distinct from the sensitive personal information threshold for risk assessments. These are not duplicative. In

		overlaps with existing requirements for biometric data under the CPRA. This duplication increases compliance costs and creates confusion without enhancing consumer privacy.	addition, to the extent these thresholds overlap for a single processing activity, it does not pose undue burden on businesses because they are only required to conduct a single risk assessment. (*See* § 7156(a).)
7150(b)(6)	504	The section enumerates when processing poses a significant risk to consumers' privacy and includes training of ADMT for a list of enumerated purposes "or profiling of a consumer." The "or" introduces uncertainty as to the intended scope of the provision. Comment recommends that profiling be included only to the extent that it is associated with activities that make a significant decision concerning a consumer.	The Agency disagrees with this comment. The term "physical or biological identification or profiling" is clearly defined, and the corresponding training threshold is clear. Comment's suggestion would be less effective than the regulation at protecting consumers' privacy because it would narrow the scope of activities covered by the threshold.
7150(b)(6)	107, 120	Comment encourages the Agency to retain the more focused approach in § 7150(b)(6), which only requires risk assessments for companies training ADMT for significant decisions or specific sensitive activities. The prior draft regulation would have required risk assessments for an extremely broad set of activities. Comment appreciates the effort to more narrowly focus on processing that is intended to train an ADMT, identity verification, or physical or biological identification or profiling.	The Agency agrees with this comment to the extent that it supports the Agency's regulations and notes the comment's support.
7150(b)(6)	132, 314, 404, 557	Comment argues that the scope of this section is too broad. It extends to information that businesses never intend to use for training ADMT or any other high-risk purpose, and therefore should be restricted to cases where the business actually intends to use the information. It should not include "permits others to use, plans to permit others to use, is advertising the marketing the use of, or plans to advertise or market the use of." This language should be removed, as it conflicts with the "intent" language and will bring in scope a wide-range of general use models that are primarily used for other, low-risk purposes. Comment also suggests eliminating the automatic categorization of training models used for ID verification data and biological identification as sensitive information. Models may be trained for such purposes	The Agency disagrees with this comment. Permitting others to use, or advertising or marketing the use of, consumers' personal information or planning to do so demonstrates a clear intent to use consumers' personal information for training purposes; it does not inappropriately encompass models used for low-risk purposes as suggested by commenter. Additionally, processing a consumer's personal information for identity verification and biological identification or emotion recognition presents significant risk to consumers' privacy, such as data leakage that can reidentify consumers whose personal information was used to train the model and a lack of transparency and consumer control over the use of their personal information for training. In addition, this threshold is distinct from the sensitive personal information threshold. To the extent these thresholds overlap

		without identifying any specific person if, for instance, they are trained on anonymized data. If the models do identify specific persons, CPRA's existing regulations for sensitive data will apply and risk assessments will still be required, as CPRA designates biometric data as a form of sensitive data. This threshold is redundant. These categorizations therefore do not enhance user privacy and in fact undermine businesses' ability to use privacy-preserving techniques in their training models. Further, the rules should not extend risk assessments to processing for training a model that is used for emotion recognition, if it does not otherwise involve identifying a specific person (which is already covered). It should also not expressly call out training for models used for biological identification. Risk assessments already extend to processing of sensitive data.	for a single processing activity, it does not pose undue burden on businesses because they are only required to conduct a single risk assessment. (*See* § 7156(a).) Further, commenter does not explain how conducting a risk assessment would undermine business's ability to use privacy-preserving techniques in their training models. The Agency does not believe this is the case. Rather, a risk assessment requires businesses to identify relevant privacy risks and safeguards before initiating the processing, which supports the use of privacy-preserving techniques in training models.
7150(b)(6)	403	Comment states the risk assessment requirements for training ADMTs are overly broad. Comment suggests that the requirements only apply when ADMT is used for a significant decision that will affect an individual and not include when a business "intends to use" ADMT. Otherwise, this creates confusion over whether research activities, such as fine-tuning models for other low-risk use cases, would trigger a risk assessment.	The Agency disagrees with this comment. The threshold is not overly broad. Training uses of personal information present significant risk to consumers' privacy, and the threshold is already limited to intent-based uses. Further, it is unclear what comment means by fine-tuning for "low-risk" use cases. Nonetheless, the Agency disagrees that any of the uses in § 7150(b)(6) are low risk.
7150(b)(6), 7153(a)	72, 155, 236, 312, 454	Comment argues that the Agency lacks the statutory authority to regulate the training of ADMT models. The CCPA only authorizes the Agency to issue regulations on the "use" of ADMT. Comment argues that training an ADMT tool should not trigger risk assessments, as this is a convoluted and unclear standard, particularly for businesses that rely on both data subject to the CCPA and data that is exempt from the CCPA to train tools. Comment requests that all references to "training AI" in the risk assessment section be removed. Comment recommends further revisions to § 7150(b)(6) concerning the use of personal information to	The Agency disagrees with this comment. The training threshold is within the Agency's authority and furthers the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment. (*See* Civ. Code § 1798.185(a)(14)(B).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) These training uses of consumers' personal information pose significant risk to

		train an ADMT. Comment argues that it is not clear what risk to privacy is posed by the training of ADMT. Restricting developers from tweaking algorithms at scale would be incredibly burdensome; it would have a disproportionate impact on smaller California firms, and also, inevitably, harm consumers' use of and experience with AI tools. Comment also argues that the definition of "intends to use" should be removed. The language about "plans" to use or permit others to use conflicts with the intentionality component of the revised text, and will bring in scope general use models that are primarily used for other low-risk purposes. Further, imposing risk assessment and consumer rights obligations to the training of ADMT is likely beyond the scope of the statute itself. Imposing heightened obligations on the processing of personal information to train ADMT is not reasonably necessary to effectuate the purpose of the underlying statute, creating potential legal challenges in the future. ADMT training does not involve decisions that concern a specific consumer. Further, § 7153(a) should be revised to safeguard confidential, proprietary, and security sensitive information. The currently drafted language is too broad and may be interpreted to compel disclosure of trade secrets, proprietary model architecture, training datasets, algorithmic logic, or sensitive information about system vulnerabilities.	consumers' privacy, such as data leakage that can reidentify consumers whose personal information was used to train the model and a lack of transparency and consumer control over the use of their personal information for training. Additionally, the regulation is necessary to clarify when a business using personal information for training purposes must conduct a risk assessment; it is also clear and is not convoluted. It provides a clear intent-based standard that identifies the types of technologies that are subject to the regulation, and addresses circumstances demonstrating intent to use the personal information for training. To the extent a business is processing consumers' personal information for the training uses described in the regulation, the business must conduct a risk assessment. Moreover, the CCPA is reasonably clear in addressing which data are subject to the CCPA, and the CCPA's exemptions apply to the regulations. With respect to § 7153(a), the regulations are necessary to ensure that businesses conducting risk assessments have the relevant facts to conduct those risk assessments. The CCPA is already clear that it does not require a business to divulge trade secrets in risk assessments; thus, an additional exception is not necessary at this time.
7150(b)(6), 7200(a)(3)	469	Comment objects to the narrowing of the scope regarding ADMT training. The recent version narrows the initial scope of coverage by replacing "capable of being used for" with "which the business intends to use for," deferring to the business's intent rather than acknowledging the inherent risk that some ADMT can be put to high-impact uses. This again makes it easier for businesses to self-certify out of risk assessment requirements by claiming they did not intend to use the resulting model for the enumerated uses when they were training the model. The list of enumerated use cases	The Agency disagrees with this comment. The intent-based standard and training uses listed continue to address processing that presents significant risk to consumers' privacy while simplifying implementation for businesses at this time. In addition, a business cannot self-certify compliance or disregard privacy harms to consumers. A business must comply with the risk assessment requirements if its activities meet one of the thresholds in § 7150(b).

		also removed "for the generation of a deepfake" and "for the operation of generative models, such as large language models." This removal effectively allows big tech to continue training large language models on any data it can access, without regard to consent or privacy harms.	
7150(b)(6), 7220(c)(5)	187	Comment argues that numerous provisions "fail[] to provide a person of ordinary intelligence fair notice of what is prohibited, or [are] so standardless that it authorizes or encourages seriously discriminator enforcement," they require significant revisions. Specifically, ADMT disclosure requirements are broad and unclear, such as those in § 7220(c)(5), without direction as to what additional information and the types of outputs generated, and it is unclear what degree of planning reflects "intent" to determine when risk assessments would be required.	The Agency disagrees with this comment. The Pre-use Notice and access ADMT requirements are clear, providing specific direction about how to provide the required information. With respect to § 7220(c)(5), the requirements and examples in § 7220(c)(5)(A)-(C) provide clarity and guidance to businesses regarding how to comply, including what additional information is specifically required and the types of outputs that may be included. Additionally, in the risk assessment requirements, the word "plan" is reasonably clear and no additional clarification is needed at this time. More broadly, the regulations as a whole provide clear standards regarding businesses' obligations.
7151	37	Comment appreciates the added flexibility regarding stakeholder involvement in the risk assessment process.	The Agency notes commenter's support.
7151	260	Comment urges the Agency to require independent evaluation of ADMT by socio-technical experts to enhance the effectiveness of risk assessments for businesses and society alike, as well as mitigate internal biases and potential conflicts of interest. With regard to § 7151(b), comment urges the Agency to include external evaluators that are free from conflicts of interest and possess domain-specific knowledge.	The Agency disagrees with this comment. § 7151(b) is clear that businesses may consult with external parties as part of the risk assessment process. This language provides clarity to businesses about what stakeholders they may consider including in the risk assessment process while providing flexibility to businesses to identify which external parties should be included in the process. The Agency does not believe mandatory independent evaluations are necessary at this time.
7151(a), 7152(a)(8)	56, 409, 505, 545	Comment argues that the revised risk assessment requirements are overly prescriptive and onerous, especially for small and mid-sized businesses. Instead of imposing rigid mandates for stakeholder involvement in assessments, the Agency should take steps to make the requirements more flexible so businesses with different kinds of internal resources (for example, small and mid-sized businesses),	The Agency disagrees with this comment. The requirements ensure that employees with necessary information to conduct the risk assessment are part of the risk assessment process. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations do not require a large expenditure of time and resources, because a business can determine how to effectively implement this requirement

		teams, and decisionmaking processes are able to conduct risk assessments that meet the requirements. The Agency should consider offering scalable guidelines that account for variations in company size and resources, ensuring that all businesses can implement reasonable stakeholder engagement. Commenter states the inclusion of which employees should participate in privacy risk assessments in § 7151 is unnecessary because companies manage governance differently and the specificity of the draft rule may not be relevant to every business. Comment argues that the regulations would require the participation of a number of individuals to conduct risk assessments that are not always needed. §§ 7151(a) and 7152(a)(8) may obligate businesses to include many employees whose "job duties" involve processing personal information, leading to large expenditures of time and resources without necessarily enhancing the quality of the risk assessment. As an alternative, the Agency should require consultation only with an individual who is primarily responsible for the processing activity, and revise the rules so businesses need not provide the name of every individual who contributed, but instead, for example, include the individual who has the authority to decide whether the business will initiate the processing. The Agency should similarly revise the regulations such that businesses need not provide the name of every individual who provided information for the risk assessment and may include, for example, 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.	based on its internal processes. The requirements are adaptable to businesses of all sizes. The comment's suggestion would be less effective than the regulation, because it would not require businesses to include relevant employees or keep track of who contributed to the risk assessment.
7152(a)	234, 239, 432	Comment urges the Agency to adjust the requirements in § 7152(a) to be less prescriptive. These voluminous requirements continue to exceed the statutory text, with no evidence that this additional information provides consumers any actual benefit. The risk assessment requirements under § 7152(a)(3) contemplate specific	The Agency disagrees with this comment. The risk assessment requirements are not overly prescriptive, but rather provide clear requirements regarding how to conduct a risk assessment that are adaptable to a variety of contexts. They also provide flexibility to businesses that comply with other frameworks, such as GDPR, because they enable businesses to leverage their

		information that does not align with the requirements of risk assessments in other laws and may not always be relevant. Businesses should have discretion to evaluate whether these elements should be evaluated as part of a risk assessment. In addition, the requirement in § 7152(a)(1) to avoid generic terms in describing the purpose of processing will be resource intensive without corresponding benefits. Indeed, this type of prescriptive requirement will be most burdensome for entities with existing risk assessment frameworks with a track record of effectiveness.	existing compliance processes to comply with the requirements in § 7152. The regulations are consistent with those other frameworks where possible while furthering the purpose and intent of the CCPA and providing clarity to businesses about their obligations. They are also consistent with the CCPA's requirement to require businesses to conduct risk assessments and ensure these assessments are comprehensive and thorough. With respect to § 7152(a)(1), it is unclear how this requirement will be unduly burdensome. A business already must be able to identify the purpose of processing in non-generic terms. (*See, e.g.*, § 7011(e).)
7152(a)	263, 471, 472, 473, 474	Comment argues that the removal of risk assessment content requirements makes the assessment of mitigation measures less robust because it no longer requires businesses to assess the extent to which the negative privacy impacts are mitigated. This change undercuts the overall goal of conducting risk assessments—to force businesses to weigh the benefits and risks of processing—which should include an assessment of how effectively the mitigation measures would decrease risks and impact the overall risk-benefit calculus. Removing the requirement that businesses identify how they will maintain knowledge of emergent risks is also counter to the interests of consumers; the Agency is effectively allowing businesses to stick their heads in the sand after system deployment, even if serious real-life harms emerge. The Agency should, at minimum, require businesses to conduct and submit the full risk assessment report by default, and correct the other deficiencies. Comment asserts that the revised rules in § 7152(a)(2)(B) no longer require businesses to test and show that their ADMT is safe for California consumers. This removal signals to businesses that they are free to deploy systems without robust policies and practices in place to ensure the quality of personal information, thus forcing consumers bear the brunt of any errors. Eliminating § 7152(a)(2) would reduce ADMT	The Agency disagrees with this comment. A business must identify the relevant benefits and risks to consumers' privacy and identify safeguards it plans to implement. This helps ensure that risks are mitigated, while simplifying implementation for businesses at this time. The regulations provide guidance to businesses about the variety of safeguards they can implement, including maintaining knowledge of emergent risks and evaluating their ADMT. A business is not limited to implementing only those safeguards, but can implement a variety of others that address the processing it is engaging in. Additionally, businesses cannot ignore real-life harms that emerge from their processing and must update the risk assessment after a material change to their processing activity. The regulations do not signal to businesses that they can deploy systems without identifying relevant risks to consumers' privacy and safeguards. It is also unclear how the regulations would allow deployment of untested and potentially dangerous ADMTs when they specifically require identification of risks and safeguards. For example, with respect to comment's concerns regarding accuracy and bias, a business must identify negative impacts to consumers from their processing, which may include inaccuracy or unlawful discrimination, as part of the risk assessment process. Further, a business can never use an ADMT for unlawful discrimination, which it can use the risk

		oversight to little more than basic recordkeeping, allowing businesses to check boxes rather than confront and address the real-world impacts of their systems. Comment argues that the revised § 7152(a)(6)(A) removes the requirement that businesses evaluate the need for human involvement and implement policies, training, and procedures to address the degree of human involvement as a potential safeguard, which also harms consumers. Every business deploying ADMTs should assess the appropriate degree of human involvement in the system to mitigate risks of inaccuracy, arbitrariness, and bias. Businesses should also consider how to properly train the humans involved so they do not give undue weight to ADMT outputs or merely rubber stamp those outputs. Comment argues that the revised § 7152(6)(B)(i) strikes the provision that would have required businesses to identify whether they evaluated the ADMT to ensure it works as intended for their proposed use and does not discriminate based on an individual's membership in a protected class. This removal allows businesses to avoid testing the system to ensure it works accurately and without discrimination before deployment. The regulations will allow businesses to deploy untested and potentially dangerous ADMTs while still attesting that they complied with the risk assessment requirements.	assessment to identify and mitigate. The risk assessment requirements are not mere recordkeeping requirements but rather ensure that businesses meaningfully identify the risks and benefits of their processing. In addition, submission of annual risk assessment information and submission of risk assessment reports upon request holds businesses accountable for conducting compliant risk assessments.
7152(a), 7156, 7157	133, 154, 512, 514, 523, 552, 553	Comment argues that the approach to risk assessments under § 7152 is overly prescriptive, leading companies to produce reports merely to satisfy the requirement rather than for its intended purpose of weighing privacy harms against benefits. It warns this formulaic approach will be unreasonably burdensome and costly for businesses and innovation, outweighing any potential privacy benefits to consumers, and is inconsistent with frameworks like the GDPR, which allow for tailored assessments. Comment argues that businesses should retain flexibility in how to approach assessments to make sure that they identify and	The Agency disagrees with this comment. The risk assessment requirements are not overly prescriptive, but rather provide clear requirements regarding how to conduct a risk assessment that are adaptable to a variety of contexts. In addition, respecting consumer privacy is not contrary to innovation; rather, the regulations foster the development of privacy-by-design products and services. Moreover, the requirements provide flexibility to businesses that comply with other frameworks, such as GDPR, because they enable businesses to leverage their existing compliance processes to comply with the requirements in § 7152. The regulations are consistent with

		weigh the right factors. Comment criticizes that the Agency has not explained how this approach will provide incremental benefits to consumer privacy. The regulations also adopt a one-size-fits-all approach, failing to take into account the wide variation in business models, risk profiles, and data practices across industries and potentially leading to unnecessary reporting burdens without meaningful consumer benefit and protection. Adherence to rigid requirements and a lack of flexibility would stifle ADMT development, use, and innovation in California. The Agency should clarify that the list of requirements is illustrative and should be applied only when relevant. For example, a business would be required to document and report numerous operational elements of its processing, including the sources of personal information, the approximate number of consumers whose personal information the business plans to process, and the names or categories of service providers, contractors, or third parties. Comment argues that the enumeration of operational elements under § 7152(a)(3), particularly §§ (D), (F) and (G), creates an excessively formulaic structure that diverts focus from substantive risk analysis. § 7152(a)(3)(D) requires businesses to approximate the number of consumers it plans to process. Particularly for a new product or service, making this assessment pre-launch is not feasible. Comment objects to § 7152(a)(3)(F) as duplicative and unnecessary since § 7152(a)(1) already covers the processing purpose, and businesses already disclose sharing practices. Comment also criticizes § 7152(a)(3)(G)(i) for focusing on ADMT methodology despite ongoing research and for not being tethered to the risk to the consumer, arguing that such risks are already addressed in other provisions. Comment recommends allowing a risk assessment that satisfies another jurisdiction's requirements to be substituted for the list of requirements in this section. Comment argues that the	those frameworks where possible while furthering the purpose and intent of the CCPA and providing clarity to businesses about their obligations. For example, the sources of personal information are necessary to identify the nature of the risk to consumers' privacy; a business using sources of personal information that a consumer may not expect or that contain inaccurate information, to make a significant decision about them, undermines consumer control over their personal information. In addition, § 7152(a)(3)(D) is feasible, as it only requires an approximate number, which a business can update when it has more information. With respect to § 7152(a)(3)(F), the types of entities to which a business discloses or makes personal information available for processing, and the purpose for that disclosure, is necessary to ensure that the business identifies the risks of the processing activity, including risks associated with that disclosure. In addition, the regulation allows businesses to identify categories of service providers, contractors, or third parties, rather than their names, which provides additional flexibility for businesses. § 7152(a)(3)(G)(i) provides clear requirements for identifying the logic of the ADMT and how it works, including its assumptions and limitations. This is necessary to identify privacy risks to consumers when using that ADMT to make a significant decision about them, and is also consistent with requirements in other jurisdictions, such as Colorado. Comment's premise that § 7152(a)(3)(G)(i) is untethered to risks to consumers is mistaken, as the risk to consumers can stem from the logic of an ADMT, such as ADMT trained on inaccurate or biased data that then uses that information to make a significant decision. With respect to allowing other jurisdictions' requirements to be utilized to meet the regulatory requirements, § 7156(b) ensures that businesses can leverage existing compliance processes while meeting the CCPA's requirements for a risk assessment. The regulations also provide an example of how a business can use an existing data protection assessment to comply with §

		text continues to require a risk assessment to include all the specific requirements under this regulation. Instead, it should follow the approach of all other state privacy laws (e.g., Colorado, GDPR) and permit businesses to rely on assessments prepared for other laws that are reasonably similar in scope and effect. The draft rules impose stricter and broader risk assessment requirements than other state privacy laws, which typically limit such assessments to sensitive data or high-risk profiling, and only allow exemptions if an existing assessment fully satisfies all requirements and covers comparable processing risks. As currently written, the draft rules contemplate interoperability only between similar "risk assessments" and do not contemplate "data protection assessments." Further, comment urges the Agency to ensure that all submitted risk assessment information remains confidential and exempt from public disclosure. Such disclosure should not waive attorney-client or work-product protections. Comment cites Colorado and Virginia laws as models and suggests California to adopt the same approach. In addition, comment criticizes the requirement to disclose employee names involved in risk assessments. This requirement is overbroad, because it would mandate disclosing all employees involved in processing personal data and would be difficult to implement. This requirement also lacks confidentiality protections and raises serious privacy concerns. Comment urges the Agency to acknowledge the risk that disclosed individuals could be targeted for their involvement or affiliation with a particular company, including for phishing or political reasons. Safeguards against public disclosure should be incorporated accordingly.	7152. The comment's recommendation would be less effective at protecting consumer privacy, because it would not ensure that businesses conduct risk assessments as set forth in the regulations. With respect to employee names, this information is necessary to ensure accuracy and accountability. Further, the risk assessment regulations do not require submission of privileged information. Additionally, providing disclosures to the Agency does not equate to it being disclosed; whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the PRA applies. The Agency is also required to comply with the Information Practices Act of 1977. (*See* Civ. Code §§ 1798–1798.78.)
7152(a)(1), 7222(b)(1)	420, 506	Comment requests the removal of the prohibition on the phrase "to improve our services" when explaining risk assessments. Comment states that removing this prohibition improves consistency and consumer communications.	The Agency disagrees with this comment. The requirement is consistent with consumer communications and existing requirements for businesses. A business already must be able to identify the purpose of processing in non-generic terms. (*See,*

		Comment requests removal of similar prohibition in communications to consumers in § 7222(b)(1). Comment urges the Agency to provide organizations flexibility to identify a range of potential improvements without identifying them granularly. The potential for new and unforeseen needs for product improvement to arise as technology and consumer interactions with products and services evolve necessitates greater flexibility.	*e.g.*, § 7011(e).) In addition, identifying a purpose in non-generic terms is necessary to identify relevant risks and benefits in a risk assessment and to ensure consumers understand how an ADMT was used with respect to them.
7152(a)(2)	121	Comment supports removing requirements to identify actions taken to maintain the quality of personal information processed by ADMT or AI, which had a vague list of actions.	The Agency notes this comment's support.
7152(a)(3)	407	Commenter states that the requirements in § 7152(a)(3) are difficult to compile and increase the risk of disclosing trade secrets through explaining the logic of ADMTs. For example, the requirement to include the approximate number of consumers may be impossible to calculate.	The Agency disagrees with this comment. § 7152(a)(3)(G)(i) provides clear requirements regarding identifying the logic of the ADMT and how it works, including its assumptions and limitations. This is necessary to identify privacy risks to consumers when using that ADMT to make a significant decision about them, and it is also consistent with other jurisdictions' risk assessment requirements, such as Colorado's. Businesses can leverage their existing compliance processes to comply with the requirements in § 7152. Further, with respect to trade secrets, the CCPA is clear that it does not require businesses to divulge trade secrets in risk assessments. In addition, it is not difficult to compile the information required by § 7152(a)(3)(D), as it only requires an approximate number, which a business can update when appropriate.
7152(a)(3)	408	Comment states that it is unclear how requirements such as the ones required in § 7152(a)(3) will be used by the Agency to improve consumer privacy when other jurisdictions and laws require assessments tailored to the processing activity.	The Agency disagrees with this comment. Each requirement in § 7152(a)(3) is necessary to ensure that businesses appropriately conduct a risk assessment that identifies risks and benefits to consumers' privacy. Further, these requirements are consistent with other jurisdictions' risk assessment requirements, such as those in Colorado. Businesses can leverage those existing compliance processes to comply with the requirements in § 7152.

7152(a)(5)	250	Comment finds the risk assessment regulations impose excessive burdens by requiring granular documentation and evaluation of highly subjective impacts, such as "psychological harms" to an "average consumer." These requirements are not only difficult to operationalize, but they also risk exceeding the statutory mandate provided under the California Consumer Privacy Act (CCPA). Financial institutions are already subject to robust risk assessment obligations under the GLBA and oversight by federal regulators.	The Agency disagrees with this comment. § 7152(a)(5) does not impose excessive burdens, but rather requires businesses to identify negative impacts to consumers' privacy from their processing activities. It also provides a non-exhaustive list of negative impacts for businesses to consider, which provides guidance for businesses regarding what these impacts, such as psychological harms, can be. With respect to authority, the Agency has authority to issue this regulation, because it is necessary to ensure businesses can identify risks to consumers' privacy from their processing activities. (*See* Civ. Code §§ 1798.185(a)(14)(B), (b), 1798.199.40(b).) With respect to financial institutions, businesses can leverage existing compliance processes to comply with the requirements of § 7152, as set forth in § 7156(b). Further, to the extent a CCPA exemption applies, such as for information subject to the GLBA and its implementing regulations, that information is not subject to the risk assessment regulations.
7152(a)(5)	599	Comment supports retaining the requirement businesses consider the potential harms to consumers before and during high-risk processing, notwithstanding the modification's narrowing.	The Agency agrees with this comment and notes the comment's support.
7153	122	Comment appreciates the current draft focuses on information-sharing obligations for companies that make ADMT to other businesses. The prior draft regulations would have required businesses that train both ADMT and AI and permit others to use it to provide a plain language explanation of limitations on the technology. Comment appreciates that the current draft focuses instead on providing the recipient business with the facts available to the original business. (§ 7153.)	The Agency notes the comment's support.
7153(b)	294	Comment argues that this section should be restored. When ADMTs are trained and made available to others, it is only	The Agency disagrees with this comment. The Agency removed the originally proposed § 7153(b) to simplify implementation for businesses at this time.

		reasonable that developers disclose key information about their data use and system limitations.	
7154	262	Comment urges the Agency to require businesses to adopt the principle of data minimization. Specifically, comment recommends that the Agency require businesses to limit data collection strictly to what is necessary for the stated purpose. One key strategy the Agency should adopt is mandating the use of Privacy-Enhancing Techniques (PETs), which help minimize data collection, anonymize personal information, and prevent unauthorized data transfers.	The Agency disagrees with this comment. § 7002 already requires that businesses' use of consumers' personal information be necessary and proportionate, and provides clear rules regarding how to do so, including requirements regarding the minimum personal information to achieve the purpose of the processing and when consent must be obtained. Regarding PETs, the risk assessment regulations provide guidance to businesses about the use of these technologies in § 7152(a)(6)(A)(ii). The Agency does not believe that mandating the use of these technologies is necessary at this time.
7154	276, 475, 540	Comment argues that the removal of the prohibition on processing personal information when the specified risks outweigh the benefits weakens risk assessment regulations. The May 2025 version weakens this into an aspirational "goal," limiting the Agency's enforcement authority and enabling businesses to continue harmful practices even when identified as high-risk. Self-certification by businesses is inadequate. Comment states that this specific revision also does not seem to fulfill the requirement laid out in the CPRA. Comment recommends that this provision is modified not only to make clear that businesses are prohibited from processing data when the risks outweigh the benefits, but to also make clear that the Agency has the formal ability to challenge businesses' assessments of the tradeoffs between the benefits of their processing activities and the harms. Comment proposes language regarding the Agency's ability to conclude that the benefits do not outweigh the processing, findings of probable cause, and the ability to hold a hearings and issue orders for violations.	The Agency disagrees with this comment. § 7154 has been revised to state the goal of a risk assessment, as specifically stated in the CCPA. (*See* Civ. Code § 1798.185(a)(14)(B).) This is necessary to provide the statutory goal of a risk assessment in the regulations, so that the requirements and goal are in one place. This improves the clarity and readability of Article 10 overall. In addition, the regulations do not allow businesses to self-certify. Businesses must conduct a risk assessment in compliance with the requirements set forth in the regulations. The comment's recommended language is not necessary. As with other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law.
7155	38	Comment appreciates the additional clarity regarding the timing for submitting an initial risk assessment, the timing for submitting an updated risk assessment following a	The Agency notes the comment's support.

		material change, what constitutes a material change, and the required retention period for risk assessment documentation.	
7155	240	Comment suggests that the Agency should make clear that risk assessments are required only for new processing activities—not those that occurred prior to the effective date of the regulations. Banks already assess their sensitive information processing under existing laws or programs, and forcing a massive audit of these activities would require a potential re-do of risk assessments. This is neither feasible, nor a desirable use of privacy resources.	The Agency disagrees with this comment. The regulations require a risk assessment for processing that presents a significant risk to consumers' privacy after the effective date of these regulations. The regulations also provide businesses with additional time to conduct risk assessments for certain processing activities to lessen their compliance burden. This approach benefits both businesses and consumers, by balancing flexibility to come into compliance with ensuring protections for processing that presents significant risk to privacy. The comment's recommendation would be less effective than the regulation, because it would not subject processing activities that present significant risk to consumers' privacy to a risk assessment so long as they began before the effective date of the regulations. In addition, to the extent that a business has already conducted a risk assessment, it can leverage its existing compliance processes to comply with the requirements in § 7152. This provides businesses with additional flexibility to come into compliance with the regulations.
7155(a)(1), (a)(3), (b), Timing	158, 188, 334, 344, 413, 414, 415, 516	Comment argues that the rules create confusion regarding the timing of risk assessments. §§ 7155(a)(1), (a)(3), and (b) contain conflicting timelines for new, continuing, and materially changed processing. These provisions are difficult to reconcile. For example, § 7155(a)(1) appears to prohibit new processing from beginning without a prior risk assessment—even though § 7155(b) allows risk assessments for pre-existing activities to be completed as late as December 31, 2027. Similarly, § 7155(a)(3) requires updates within 45 days of a material change, but that presumes the existence of an initial assessment, which may not yet be required under § 7155(b). Comment recommends extending the risk assessment deadline to December 31, 2027, for all	The Agency disagrees with this comment. The regulations are clear. Businesses must complete their risk assessments before initiating a processing activity as set forth in § 7150(b). The December 31, 2027, deadline only applies to processing that began before the effective date of the regulations and that continues after that effective date.. This extension of time to complete the risk assessment benefits businesses by giving them additional time to work through potential backlogs of processing activities. This extension is not necessary for new processing that begins after the effective date of the regulations, because there would not be a similar backlog to work through. Further, the regulations clearly indicate when an update to the risk assessment is necessary. Once a business has

		processing initiated before that date. Comment also recommends any new processing after that date require a risk assessment before initiating it, and for material changes after December 31, 2027, requiring an update within 45 calendar days. Comment states that the regulations should be revised to make clear the requirements for processing activities engaged in before the date on which risk assessments begin, for new processing activities initiated after that date, and material changes. Additionally, even assuming the regulations are finalized by the end of 2025, the regulations provide businesses little time to come into compliance. The requirements in the regulations, such as the ADMT opt-out requirements, have changed substantially over the course of the rulemaking process, and the requirements will demand substantial time and engineering resources. To allow businesses with sufficient time to come into compliance with the requirements reflected in the regulations, the Agency must update all timelines, including for provisions in the regulations that modify existing privacy regulations, to enter into effect 24 months after the regulations are finalized.	conducted a risk assessment and there is a material change to the processing activity, the business must update that risk assessment as set forth in § 7155(a)(3). The comment's recommendations would be less effective than the regulation at protecting consumer privacy, because they would not require risk assessments prior to initiating new processing activities until 2028. With respect to timing more broadly, in response to the initial public comments, the Agency revised the regulations to provide businesses with additional time to come into compliance with the ADMT regulations in § 7200(b) and to provide a phased implementation period for cybersecurity audits in § 7121(a). Further, the risk assessment regulations provide businesses with additional time to conduct risk assessments for certain processing under in § 7155(b). The Agency has determined that the time periods provided for in the regulations appropriately balance protecting consumer privacy while providing businesses with a reasonable amount of time to come into compliance. Further delaying the date by which businesses must come into compliance with the regulations is not necessary at this time.
7155(a)(2), 7157(b)(3)-(b)(4)	502, 546	Comment argues that the regulations include some requirements that add administrative burden without corresponding privacy benefits for consumers, such as § 7157(b)(3) and § 7155(a)(2). For example, the obligation set forth in § 7157(b)(3) to submit to the Agency information about the number of risk assessments conducted or updated for each processing activity would require businesses to link each risk assessment to individual processing activities, even though processing activities may cross over multiple risk assessments and a single risk assessment may cover multiple processing activities. In addition, the obligation set forth in § 7155(a)(2) to review and update as necessary all risk assessments would impose undue burden in light of the obligation to update the assessment where there are	The Agency disagrees with this comment. The regulations balance privacy protections for consumers and flexibility for businesses to come into compliance. With respect to §§ 7157(b)(3)–(4), this requirement is not unduly burdensome, because businesses already have this information available. In addition, it is necessary for the Agency to identify how many risk assessments businesses conducted each year, which processing activities triggered more or less risk assessments, and what categories of personal information and sensitive personal information are involved in the processing activities that require a risk assessment. (*See, e.g.,* Civ. Code § 1798.199.40(d).) With respect to § 7155(a)(2), this requirement is necessary to clarify that risk assessments address risks to consumers' privacy throughout a processing activity's lifecycle

		material changes in processing practices set forth in § 7155(a)(3). One comment asks the Agency to remove the requirements regarding the need to report per-category personal data (§7157(b)(4)), link risk assessments to each processing activity (§7157(b)(3)), and review all assessments (§7155(a)(2)) rather than just when processing changes. Comment suggests striking § 7157(b)(4) and § 7155(a)(2) in their entirety and editing § 7157(b)(3) to delete the language "in total and for each of the processing activities identified in section 7150, subsection (b)."	and do not reflect out-of-date information. This approach is consistent with approaches taken by the Colorado Privacy Act and the EU's GDPR.
7155(a)(3), (b)	57	Comment argues that the regulations set an unrealistic timeline for updating risk assessments. Businesses are given over two years to complete their initial risk assessments (with a December 31, 2027, deadline for completion), yet only 45 days to update them following a material change in processing. This is an insufficient timeframe, considering the complexity of the regulations and scope of the risk assessment requirements. The Agency should update the rules to allow for a more reasonable update period to complete relevant updates in the event of material changes to relevant processing practices. Such a change would allow businesses to conduct thorough updates to assessments without being rushed by an unnecessarily short 45-day timeline for completion.	The Agency disagrees with this comment. Commenter appears to misread the regulations. Businesses must complete their risk assessments before initiating a processing activity set forth in § 7150(b). The December 31, 2027, deadline only applies to processing that began before the effective date of the regulations and that continues after that effective date, as set forth in § 7155(b). Further, with respect to updating the risk assessments, up to 45 days is a reasonable timeline. A business would already have conducted the risk assessment, and would only be updating it to address the material change at that point. The Agency has determined that changing the number of days by which an update must be completed is not necessary at this time.
7156	124, 152, 410, 432, 507, 511, 524	Comment argues that § 7156 allows reuse of other risk assessments only if fully equivalent to CPPA requirements, which is redundant. It undermines the benefits of interoperability because companies must submit every additional data requirement included by California. Comment argues that § 7156(b) neuters the safe harbor provision because the revised rules' required content for risk assessment does not align with any other similar privacy law framework for risk assessments, notwithstanding the flexible statutory text. Risk assessment requirements should be	The Agency agrees in part with this comment that there are benefits to consistency and interoperability with other privacy frameworks and that businesses should be able to leverage risk existing risk assessments. The Agency otherwise disagrees with this comment. § 7156(b) ensures that businesses can leverage existing compliance processes while meeting the CCPA's requirements for a risk assessment. The comment's recommendation to allow the use of reasonably similar risk assessments would be less effective at protecting consumer privacy, because it would not require businesses to conduct risk

		interoperable with other global frameworks (*e.g.*, NIST CSF) and other state regimes, and should embody flexibility rather than prescriptiveness. Comment believes the regulations are overly prescriptive and fail to accommodate different business models or leverage existing risk assessments from other jurisdictions. Adherence to rigid requirements and a lack of flexibility would stifle ADMT development, use, and innovation in California and would result in resources being diverted to paperwork. Comment asks for recognition of "reasonably similar in scope and effect" assessments. The Agency should consider a more flexible approach to allow a business to rely on a single risk assessment for similar and interconnected processing activities across states, provided that all substantive elements are included. Interoperability mechanisms for risk assessment obligations are extremely impactful as they allow businesses to harmonize compliance and technical processes and avoid procedural burdens, without impacting the level of privacy and security afforded to individuals.	assessments as set forth in these regulations developed based on the CCPA requirements and would provide less clarity to businesses regarding when an existing risk assessment complies with these requirements. Further, it is unclear what commenter means by "provided that all substantive elements are included," as a risk assessment that includes the requisite elements in § 7152 of these regulations would be compliant. The regulations also provide guidance to businesses for additional clarity. § 7156(b)(1) provides an example of how a business can use an existing risk assessment to comply with § 7152. These requirements provide flexibility to businesses and accommodate different businesses processes. The Agency does not believe that additional clarification is necessary at this time.
7157	39, 369	Comment supports the Agency's modifications to the submission requirements in § 7157. Comment had raised concerns about unabridged risk assessments required in the original text resulting in the disclosure of confidential business information. Such a requirement would have also added significant compliance costs to the risk assessment process to create different versions of the same information. Providing abridged risk assessments also created serious confidentiality challenges and would have resulted in an unmanageably large amount of information for the Agency to process and retain. Therefore, comment is appreciative of the Agency's removal of this requirement. Comment also supports the Agency's revisions to streamline requirements relating to risk assessment review and certification.	The Agency notes commenter's support.

7157	128, 153, 433	Comment recommends confidentiality protections for risk assessment materials provided to the Agency. Comment recommends a new provision to state that risk assessment materials disclosed to the Agency are to be treated as confidential by default and are exempt from open records laws. In addition, comment requests language that providing materials to the Agency does not constitute a waiver of attorney-client privilege, work product protection, or other applicable protections. Comment recommends the regulations include the same protections that all other state privacy laws include with their risk assessment provisions. This is consistent with the CCPA's text itself, which guarantees that the risk assessment shall not require "a business to divulge trade secrets." Comment also asserts that this would align with other California legislative practices.	The Agency disagrees with this comment. The risk assessment regulations do not require the submission of privileged information. Additionally, providing disclosures to the Agency does not equate to it being disclosed; whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the PRA applies.
7157	251	Comment suggests that the Agency should expressly clarify that no provision requires a business to reveal trade secrets or other intellectual property. Comment also recommends adding a confidentiality clause similar to the one proposed for cybersecurity audits, ensuring that risk assessments submitted to the Agency remain protected and proprietary.	The Agency disagrees with this comment. The CCPA already provides appropriate trade secret protections, and additional regulations are not necessary at this time.
7157	295, 476, 583	Comment suggests that businesses should be required to provide full, unredacted risk assessments to the Agency or Attorney General when requested. Transparency here supports both enforcement and accountability. Comment argues that the May 2025 proposal requires businesses to report little information to the Agency, reducing the Agency's ability to assess the adequacy of risk assessments. The proposal also would provide very little information for the Agency to include in a public report. The requirements only require self-certification, which does not protect consumers. Comment suggests that the Agency should reinstate the November 2024 version of risk assessment requirements	The Agency disagrees this comment, to the extent it recommends modifications to the regulations. The submission provisions require businesses to submit relevant risk assessment information and reports to the Agency while providing those businesses with flexibility to come into compliance. For example, the annual risk assessment information provides necessary information for the Agency's reporting and other functions. The Agency removed the annual submission of abridged risk assessments to simplify implementation for businesses at this time. Further, risk assessments are submitted to the Agency, not the public more broadly. The Agency can use the information to create a public

		and require businesses to make public (at a minimum) the abridged risk assessment. Comment criticizes the limited disclosure of risk assessments. Comment recommends making risk assessments public when the Agency requests them.	report and disagrees that the information received is insufficient or would allow self-certification. Businesses also must submit their risk assessment reports to the Agency or Attorney General upon request. In addition, a business must always comply with the risk assessment requirements. Together, these requirements ensure transparency, enforcement, and accountability.
7157	412	Commenter requests that the information protection language used throughout the regulations be included in the risk assessment reporting requirements in § 7157 to create a consistent standard. This creates a consistent standard of information security across all interactions between companies and the Agency.	The Agency disagrees with this comment. It is unclear what language the comment is referring to. The Agency does not believe that additional changes to the regulations are necessary.
7157(b)	123, 127, 135, 555	Comment argues that it is unclear how the Agency will use submitted information. Comment recommends limiting risk assessment submission requirements to sensitive data processing only. Alternatively, comment seeks to limit the substance to metrics, i.e. the number of assessments. Companies are otherwise required to disclose in their privacy notice the types of personal data that they collect, process, and share. It is unclear how adding this to the submissions to the Agency will produce any greater benefit for the Agency. Comment opposes the requirement to list specific categories of personal or sensitive personal information in submitted risk assessments. Comment recommends deleting relevant language in § 7157(b)(4) or replacing the submission requirement to identify each of the categories of personal information identified in the CCPA with a higher-level requirement to state whether personal information or sensitive personal information was processed.	The Agency disagrees with this comment. The CCPA requires that businesses submit risk assessments to the Agency and that the Agency provide a public report summarizing the risk assessments submitted to the Agency. Submission of the types of personal information processed support the Agency's reporting and other functions. Additional modifications to the regulations are not necessary. The comment's suggestion to limit risk assessment submissions to sensitive data processing would be less effective at protecting consumer privacy. Processing can present significant risk to consumers' privacy even if no sensitive personal information is involved. Submission of risk assessment information and reports to the Agency is necessary for all processing activities that present significant risk to consumers' privacy.
7157(b)	156, 411, 525, 554	Comment states that prescriptive and detailed disclosures, such as in § 7157(b), raise compliance costs and give consumers inconsistent experiences depending on their jurisdiction. Submitting metrics tied to low-risk processing	The Agency disagrees with this comment. With respect to limiting risk assessment submissions, this would make the regulations less effective at protecting consumer privacy. Processing can present significant risk to consumers' privacy

		imposes a high compliance cost without commensurate privacy benefit. The Agency should consider limiting this obligation to a subset of high-risk activities, such as processing or selling sensitive personal information and the use of ADMT to make a legally or similarly significant decision. Comment also suggests the Board evaluate the list of specific requirements to focus on functional data with clear utility and harmonize requirements with other jurisdictions. Additionally, the Agency should clarify that metrics submitted under § 7157 may be aggregated and need not include consumer-specific information or granular processing disclosures. Comment objects to mandatory submission, arguing that the annual submissions are burdensome, inconsistent with other laws, and may lead to reduced privacy protections because businesses may prepare assessments in a way that is legally protective. The CPRA statute mandates that the Agency issue regulations that require submission at a regular cadence, which allows the Agency to set separate standards for submission. Further, the rules require companies to submit risk assessments in the employment context to the regulator, but in most instances, any decisions in the employment context are confidential and not available to competitors. Comment asks for an exception to not require the submission of information that is confidential business/trade secret information.	even if neither sensitive personal information nor the use of ADMT is involved. Submission of risk assessment information and reports to the Agency is necessary for all processing activities that present significant risk to consumers' privacy. Further, the information to be submitted to the Agency is necessary for the Agency's reporting and other functions. it While the Agency strives for harmonization with other jurisdictions as appropriate, it must implement the CCPA's requirements and further the intent and purposes of the statute. Regarding metrics submissions, the risk assessment information requirements are already clear about what information needs to be submitted to the Agency annually, and they do not require granular disclosures; the Agency does not believe that additional modifications are necessary. Further, annual submission of risk assessment information to the Agency ensures continual compliance with the requirements by businesses and promotes consistency across the risk assessment and cybersecurity audit regulations. In addition, the CCPA is already clear that it does not require businesses to divulge trade secrets in risk assessments; additional regulatory exceptions are not necessary.
7157(b)(5), (b)(6), (c)	58, 125, 509	Comment argues that the regulations would impose strict executive accountability requirements. They would require a member of the business's executive management team to sign an attestation certifying the correctness of the risk assessment under penalty of perjury. This is an extreme measure that introduces the potential for personal legal liability. The Agency should remove this signed attestation requirement from the risk assessment rules. Comment argues that the requirement could have the unintended	The Agency disagrees with this comment. The attestation requirement ensures accountability at the highest levels of the businesses. In addition, attestation under penalty of perjury is necessary to ensure that businesses submit truthful and accurate information to the Agency.

		effect of deterring otherwise qualified individuals from leading data privacy management programs. The Agency could address this concern while preserving accountability by requiring attestation that the information is correct "to the best of [the individual's] knowledge" and removing the reference to perjury.	
7157(e)	59	Comment argues that the regulations grant the CPPA unrestricted power to request risk assessment reports at any time, with no limits on how often the Agency may make such requests. Businesses would be required to submit reports within 30 days of a request, which is a rigid and demanding deadline. This unrestricted submission requirement also raises potential legal risks. Businesses must be allowed to preserve attorney-client and work product protections when submitting risk assessments to the Agency. Without these safeguards, they could be forced to disclose sensitive legal analyses and proprietary information.	The Agency disagrees with this comment. The risk assessment report does not require privileged information, so additional safeguards are not necessary. In addition, the CCPA requires that businesses submit risk assessments to the Agency. The submission requirements reduce the burden on businesses by requiring annual submission of risk assessment information, and submission of risk assessment reports upon request. The 30-day submission upon request is reasonable, incorporates feedback from public comments, and is consistent with other jurisdictions, such as Colorado.
RAs	3	Comment supports the recognition that risk assessments are distinct from audits and should not be standards-driven. Comment emphasizes that risk assessments are an internal exercise, often done under client privilege with a third-party firm, and businesses should not be required to submit risk assessments to the CPPA.	The Agency notes commenter's support. With respect to submission, the CCPA requires that businesses submit risk assessments to the Agency. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. With respect to privilege, the regulations do not require the submission of privileged information.
RAs	151, 399, 406	Comment appreciates the Agency's decision to make several improvements to the risk assessment framework but argues that the regulations continue to present several legal, operational, and interoperability challenges that require further modification to avoid undermining their stated purpose. Comment states that the requirements are overly burdensome and increase the cost of compliance for companies.	The Agency disagrees with this comment. The regulations provide clear requirements for businesses and enable businesses to leverage their existing compliance processes while complying with the CCPA's requirements. The regulations also further the intent and purposes of the CCPA. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The Agency has determined that further modifications are not necessary.
RAs	446	Comment argues that the regulations do not adequately address the unnecessarily low threshold and the prescriptive	The Agency disagrees with this comment. The regulations require risk assessments for processing that presents significant

		nature of the required risk assessments that provide limited benefit to consumers. The threshold does not align with other existing risk assessment frameworks, nor does it align with the other sections of the regulations. Comment urges the Agency to adopt a standard that would require a risk assessment for activities that are "likely to result in a high risk to the rights and freedoms of natural persons" as is similarly required under the GDPR. This approach would be more consistent with the revised ADMT scope and would focus regulatory burden on high-risk activities.	risk to consumers' privacy, consistent with the CCPA's requirement. The regulations are also consistent with other frameworks, such as the GDPR and Colorado Privacy Act. The regulations are also flexible and adaptable to a variety of contexts. The regulations also allow businesses to leverage their existing compliance processes when conducting risk assessments.
RAs	470	Comment argues that the regulations fail to require an analysis of the benefits and risks of processing. Only some of these components are required components of the "risk assessment report." Several important components of a risk assessment, including an assessment of the benefits of the proposed processing and an assessment of the privacy risks of the processing, are not required to be included in the risk assessment report, thus undermining the goal of risk assessments. The exclusion of the benefits and privacy risks of processing from the risk assessment report runs counter to the text of the CCPA, stymies the goal of risk assessments, and undercuts the Agency's oversight authority. The Agency is diminishing its own ability to gain insight into privacy risks of processing activities that businesses would have had to disclose.	The Agency disagrees with this comment. The regulations provide clear requirements, with guidance provided as necessary, and ensure that businesses identify relevant benefits, risks, and safeguards for a given processing activity. The goal of the risk assessment is explicitly stated in § 7154. Further, the risk assessment report provides necessary information to the Agency while simplifying implementation for businesses at this time. As with other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law.
RAs	600, 601, 602	Comment recommends explicitly encouraging businesses to additionally consider cybersecurity risks posed by the processing activity in addition to privacy impacts, such as the likelihood and severity of potential security incidents associated with processing, misuse, or unauthorized access. Comment recommends businesses be required to assess risks from the business's supply chain. Controls of service providers that play a role in high-risk processing must be factored into the risk analysis. Comment encourages the	The Agency disagrees with this comment to the extent that it suggests that the regulations do not address cybersecurity risks. Both the negative impacts and safeguards may be considered by businesses to address cybersecurity. In addition, the regulations are clear that these are non-exhaustive, and a business may consider other privacy risks and safeguards. Further, as part of conducting the risk assessment, a business must identify relevant service providers, contractors, or third parties in the processing, which enables the business to identify relevant risks from involving those parties and corresponding

		Agency to recommend businesses leverage automated or continuous risk assessment tools to automatically update risk levels as conditions change, detect changes in real-time, and keep regulations forward-compatible.	safeguards. This addresses comment's concern regarding assessment of risks from a business's supply chain and service providers. With respect to automated or continuous tools for updating risks assessment, the Agency has determined these are not necessary at this time. Businesses must update their risk assessments after a material change in the processing and review them for accuracy and make any necessary changes every three years. These requirements ensure that risk levels are updated while limiting the burden on businesses.
RAs	68	Comment urges the Agency to continue refining the regulations with an eye toward contextual, risk-based rules that protect individuals while encouraging beneficial innovation. Comment strongly supports the need for interoperability in risk assessment requirements across states, at the federal level, and among like-minded international jurisdictions. Comment argues that the approach outlined in the rules are overly prescriptive, and the Agency has not demonstrated how this duplicative requirement provides meaningful additional privacy protections.	The Agency disagrees with this comment. The risk assessment requirements are not overly prescriptive or duplicative. Rather, they provide clear requirements regarding how to conduct a risk assessment that are adaptable to a variety of contexts. They also provide flexibility to businesses that comply with other frameworks, such as GDPR, by enabling businesses to leverage their existing compliance processes to comply with the requirements in § 7152. The regulations are consistent with those frameworks where possible while furthering the purpose and intent of the CCPA and providing clarity to businesses about their obligations. The regulations support both privacy protections and innovation, and ensure that businesses meaningfully identify benefits, risks, and safeguards.
RAs	480	Comment rejects industry claims that risk assessment reporting is overly burdensome. It asserts that most businesses already perform such assessments in other states and jurisdictions. Moreover, assessments actually promote compliance. These assessments will help businesses comply with CCPA provisions like § 7002, which limits data collection to what is necessary, and § 7027, which empowers consumers to restrict the use of sensitive personal information.	The Agency agrees with this comment and notes its support.
RAs	494	Comment suggests that the concept of "profiling" being subject to heightened regulatory obligations should be limited to activities that effectuate a significant decision	The Agency disagrees with this comment. The regulations provide clear thresholds for when a risk assessment is required in § 7150(b). The thresholds are consistent with the CCPA's

		concerning a consumer. The current scope would extend risk assessment requirements to many beneficial profiling decisions that do not present significant risk to consumers' privacy and security, thereby burdening businesses with compliance processes that do not provide meaningful privacy and security protections. This approach contravenes the statutory requirement to issue regulations requiring risk assessments for processing that presents significant risk. As drafted, businesses would need to complete risk assessments for low-risk profiling decisions, such as predicting a person's font or music preferences. The current definition is also likely to capture longstanding, uncontroversial workplace systems that do not replace human decisionmaking, make significant decisions, or pose any consumer privacy risk, such as systems tracking production or employee reliability.	requirement to require risk assessments for processing that presents significant risk to consumers' privacy. This includes the use of ADMT for significant decisions, certain automated processing, and certain training uses of personal information.

ARTICLE 11. AUTOMATED DECISIONMAKING TECHNOLOGY

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7200	280	Comment criticizes the removal of behavioral advertising from ADMT requirements. Advertising in general has also been removed from the scope of the requirements for ADMTs. This change means that the requirements for ADMTs do not apply to ADMTs used to deliver advertising related to a significant decision. This will enable businesses to continue using, without any meaningful safeguards, behavioral advertising to determine – and limit – who receives advertisements about employment, housing, and other critical opportunities and services. The regulations no longer address the use of personal data to prevent different groups of consumers from learning of and pursuing available opportunities and services. The Agency should restore the	The Agency disagrees with this comment. The Agency removed the behavioral advertising threshold and revised the definition of "significant decision" to exclude "advertising to a consumer" to simplify implementation for businesses at this time. The regulations continue to balance protecting consumers' privacy and simplifying implementation for businesses as this time.

		definitions and coverage of advertising and significant decisions in the previous version of the proposed rules.	
7200	573	Comment argues that the scope of covered ADMT under § 7200 should not include profiling of a consumer, or at minimum, should exclude behavioral advertising. If not, then the draft should at minimum not apply the access right to this type of ADMT processing.	The Agency disagrees with this comment. The CCPA is clear that ADMT includes profiling. To the extent a business is using ADMT to make a significant decision, it must comply with Article 11. The comment also appears to refer to the proposed text published on November 22, 2024, not to the modified text of proposed regulations published on May 9, 2025. The modified text of proposed regulations published on May 9, 2025, reflects that the Agency removed profiling for behavioral advertising and other extensive profiling thresholds from Article 11's requirements.
7200(a)(1)	136	Comment recommends limiting this section to the hiring and firing of employees.	The Agency disagrees with this comment. The Agency considered the types of decisions that have important consequences for consumers and present significant risk to their privacy and determined that all of the following meet those criteria: hiring; allocation or assignment of work for employees; salary, hourly or per-assignment compensation, incentive compensation such as a bonus, or another benefit; promotion; and demotion, suspension, and termination. The regulations balance protecting consumers' privacy and simplifying implementation for businesses as this time. The comment's suggestion to limit this section to the hiring and firing of employees is not more effective or appropriate than the regulation adopted by the Agency.
7200(a)(2)	559, 560, 561	Comment argues that §§ 7200 (a)(2)(A)–(C) should be limited in scope.	The Agency agrees with this comment to the extent that it supports the Agency's regulations. The comment appears to refer to the proposed text published on November 22, 2024, not to the modified text of proposed regulations published on May 9, 2025. The modified text of proposed regulations published on May 9, 2025, reflects that the Agency removed previous §§ 7200(a)(2)(A)–(C) from Article 11's requirements to further simplify implementation for businesses at this time.

7200(b)	41	Comment argues that the proposed January 1, 2027, compliance deadline for businesses that use ADMT for significant decisions prior to that date is not feasible. ADMT is a developing and evolving technology, and the Agency should provide ample time for affected entities to comply with any regulatory requirements. Comment requests that the Agency postpone the compliance date by at least one year to January 1, 2028.	The Agency disagrees with this comment. The compliance dates balance the burden on businesses with protections for consumers' privacy. Additional time for compliance would be less effective at protecting consumers' privacy and ensuring they can meaningfully exercise their CCPA rights as soon as feasible.
7200(b)	83, 137, 165, 315, 417, 457, 526, 558	Comment states that the regulations seek to require businesses to perform risk assessments where ADMT was used before the effective date of January 1, 2027. This creates retroactive compliance obligations that are unclear, burdensome, and difficult to implement. A business should not have to provide a risk assessment where ADMT was used prior to an effective date and is not used on or after the effective date. The first sentence in § 7200(b) should be removed to prevent confusion for businesses.	The Agency disagrees with this comment. § 7200(b) addresses Pre-use Notice, opt-out, and access right for uses of ADMT for significant decisions. It is Article 10 that sets forth the risk assessment requirements, including specific compliance dates. (*See* § 7155.) Additionally, businesses must conduct a risk assessment prior to using ADMT for a significant decision. To the extent a business initiated the use of ADMT for a significant decision before the effective date of the regulations and this continues after that effective date, the business must conduct the risk assessment no later than December 31, 2027, under § 7155(b). This balances the need for businesses to identify and mitigate risks for these activities while giving those businesses sufficient time to work through backlogs of processing activities., Further, § 7200(b) makes clear that a business using ADMT prior to January 1, 2027, must be in compliance with Article 11's requirements for opt-out of ADMT and access ADMT rights no later than January 1, 2027. The Agency has determined that no further clarification is needed at this time.
7201	536	Comment urges restoring § 7201 from the April 2025 draft, which required evaluation of physical/biological profiling systems for efficacy and discrimination to prevent real-world harms. The previous requirements to evaluate and implement practices to prevent unintended consequences and unlawful discrimination were reasonable and not overly burdensome.	The Agency agrees with this comment to the extent that it supports further protections for consumers' privacy. Nevertheless, the Agency deleted § 7201 to simplify implementation at this time. The Agency will monitor the need for additional protections for consumers' privacy as businesses come into compliance with these regulations.

7220	42	Comment argues that requirements in §§ 7220(b)(2) and (c)(1), which require pre-use notices to include language regarding when businesses plan to process personal information using ADMT and the specific purpose for which businesses plan to use ADMT, are overly broad and should be removed.	The Agency disagrees with this comment. § 7220(b)(2) is not overly broad. It provides clarity regarding when a Pre-use Notice must be provided to a consumer. Without this provision, the regulations would be less clear and less effective, because businesses would not know when a Pre-use Notice needed to be presented to a consumer. Similarly, § 7220(c)(1) is not overly broad and instead provides clarity to businesses regarding how to provide relevant disclosures to a consumer about the business's purpose of using ADMT. These requirements ensure that consumers have meaningful information about the use of ADMT so they can decide whether to exercise their opt-out of ADMT and access ADMT rights before the business uses ADMT with respect to them.
7220	109, 458	Comment argues that the regulations impose a pre-use notice, access right, and opt-out right in multiple ways that conflict with consumer protection best practices. The in-your-face notice in § 7220(c)(5) has been rejected by other U.S. state privacy laws due to concerns over consumer notice fatigue, even for more invasive practices than ADMT training. Requirements for pre-use notices will also likely result in over-notification to consumers. Pre-use notices to consumers must include at least seven specific explanations. That will result in lengthy notifications that consumers may be unlikely to read, undermining the protections created in the proposed regulations. Also, the notice requirements compel businesses to disclose judgments about outputs, potentially regulating expressive content and compelling protected speech, which the Legislature likely tried to avoid by limiting rulemaking to how notice is provided, and not what it must contain. We strongly recommend narrowing the information required in pre-use notices, so that notices are effective in alerting consumers about processing that may create concerns, not routine and expected processing.	The Agency disagrees with this comment. The notice requirements are necessary to ensure that consumers have relevant information to meaningfully exercise their opt-out of ADMT and access ADMT rights. They also provide flexibility for businesses in how to provide the relevant notices, such as combining or consolidating notices as set forth in §§ 7220(a), (e). The Agency does not believe the regulations will lead to notice fatigue but rather will ensure necessary transparency and control for consumers over their personal information. The regulations also do not compel judgments, but rather require the disclosure of limited, necessary information for consumers to understand how an ADMT would be used with respect to them.

7220	70, 138, 212, 563	Comment believes that the CPRA does not permit regulations on pre-use notice of ADMT—instead, § 1798.185 calls for regulations "governing access and opt-out rights," with respect to ADMT. At minimum, pre-use notice should be limited to where the ADMT processing is otherwise subject to access and opt-out rights. To the extent that one of these customer rights does not apply (e.g., relying on security or fraud prevention exception), then the business should not have an obligation to post this notice. In other words, § 7220(a) should apply subject to the exceptions in § 7221(b) and § 7222(a)(1). Forcing businesses to disclose how they use ADMT to perform the specified functions risks undermining the security of consumers and businesses, and requirements to make such disclosures should be minimized. Comment suggests amending § 7220(a) as follows: A business that uses automated decision-making technology as set forth in section § 7200, subsection (a), and subject to the exceptions in section § 7221(b) and section § 7222(a)(1), must provide consumers with a Pre-Use Notice. Comment states that the new language about consolidated or contextual notices is a step in the right direction, but advocates for flexibility in how notices and opt-out choices are presented, to allow integration into user-friendly interfaces rather than one-size-fits-all banner notices.	The Agency disagrees with this comment. The Pre-use Notice requirements are within the Agency's authority and are necessary to ensure that consumers have relevant information about use the of ADMT to meaningfully exercise their CCPA rights. (*See* Civ. Code §§ 1798.185(a)(15), (b), 1798.199.40(b).) In addition, comment's recommendation seems to misread the regulations. A business that is subject to an opt-out exception must still provide relevant disclosures in the Pre-use Notice, including, for example, the exception it is relying on to not provide the opt-out or how to submit an appeal of a significant decision. In addition, a business must always provide the information required in § 7222(b) in response to a request to access ADMT. However, it is not required to provide trade secret or certain security, safety, and fraud prevention information set forth in § 7222(c) when providing those disclosures. Further, it is unclear how a Pre-use Notice would undermine security. The disclosure requirements are not about security, and the regulations explicitly provide an exception for disclosing certain security information in § 7220(d)(2). The regulations also provide flexibility for businesses to combine or consolidate notices in §§ 7220(a) and (e). They balance providing consumers with necessary disclosures with flexibility for businesses in how to provide those disclosures.
7220	166, 178, 332, 423	Comment argues that the Agency has no statutory authority to require businesses to publish a "pre-use notice" for ADMT and that this prescriptive requirement substantially increases the cost of the regulations with no demonstrated benefit for consumers. Because the information required to be included in the pre-use notice is highly technical, businesses would need to make careful legal judgements about how to comply with the requirements without exposing sensitive information that has a significant impact on the ability of California innovators to compete in the global innovation race. The addition of an exception for trade secrets in certain	The Agency disagrees with this comment. The Pre-use Notice requirements are within the Agency's authority and are necessary to ensure that consumers have relevant information about use the of ADMT to meaningfully exercise their CCPA rights. (*See* Civ. Code §§ 1798.185(a)(15), (b), 1798.199.40(b).) In addition, the Pre-use Notice will not lead to overlapping or burdensome obligations. It requires disclosing a limited set of information regarding the business's use of ADMT for a significant decision so that consumers can exercise their CCPA rights to opt-out of ADMT or access ADMT. The regulations also provide flexibility for businesses to combine or consolidate

		sections does not cure that problem, as businesses still must grapple with difficult, fact-specific judgments to reconcile safeguarding trade secret-protected information with pre-use disclosure requirements. Prohibition of standard business terms such as "to improve our services" is overly restrictive. These notices could force disclosure of trade secrets or sensitive information. The Pre-use notice requirements must be removed or revised to reflect the limits set by Civil Code § 1798.185. This also will result in overlapping obligations without a clear legal basis and risk confusing consumers. Risk concerns are better addressed through assessments or reviews and not disclosures.	notices in §§ 7220(a) and (e). They balance providing consumers with necessary disclosures with flexibility for businesses in how to provide those disclosures. With respect to trade secrets, the Agency disagrees. The trade secrets provision provides appropriate protections for trade secrets while requiring that consumers receive necessary disclosures to exercise their CCPA rights. Businesses have been able to balance these considerations in providing required notices under existing California law and can continue to do so for Pre-use Notices. With respect to the phrase "to improve our services," it is unclear how this requirement will be unduly burdensome. A business already must be able to identify the purpose of processing in non-generic terms. (*See, e.g*., § 7011(e).) Further, it is unclear how assessments or reviews could replace the Pre-Use Notice in ensuring that consumers receive this information.
7220	206, 212	Comment appreciates the removal of some burdensome pre-use notice requirements in the revised draft. However, it expresses a preference for full elimination of pre-use notices but states it is most critical that it can protect proprietary logic under the existing trade secret exemption.	The Agency notes the comment's support.
7220	270	Comment argues the pre-use notice requirements are redundant in the financial services industry, where consumers already receive detailed disclosures during application processes. The customer knows how the financial institution will use their personal information – i.e., to obtain a mortgage. In addition, when a customer files an application, they receive numerous disclosures regarding the financial product and service, including the information on the NPI that will be processed in connection with an application, such that providing customers with another disclosure may be repetitive. Further, if a customer is already receiving numerous disclosures in connection with the product or service, one more notice would be lost in all the paper and not have much impact.	The Agency disagrees with this comment. The comment appears to misread the regulations. The Pre-use Notice provides consumers with relevant information to exercise their CCPA rights to opt-out of ADMT and access ADMT, including how the ADMT works to make a significant decision about them and how the significant decision would be made if a consumer opts out. The comment's examples do not address this information and would not provide the necessary information for consumers to exercise their CCPA rights. Further, the regulations enable businesses to combine or consolidate notices in §§ 7220(a), (e), which addresses comment's concern regarding consumers receiving numerous disclosures.

7220	306	Comment generally supports this subsection (d) but believes that the expansiveness of (c)(5) will make it difficult for businesses to accurately assess what information falls into these enumerated categories.	The Agency disagrees with this comment to the extent it suggests that § 7220(c)(5) is difficult to comply with or overly broad. § 7220(c)(5) is necessary to ensure that consumers have meaningful information about how the ADMT works to make a significant decision and how that decision would be made if a consumer opts out. These are tailored requirements that address how the ADMT processes consumers' personal information, the type of output generated and how that output is used to make the decision, and what the alternative process is for making that decision if a consumer opts out. The regulations also provide guidance to businesses regarding how to provide the necessary information to consumers, which further simplifies compliance. For example, § 7220(c)(5)(A) is clear that when providing the required information about how the ADMT processes personal information, businesses must include the categories of personal information that affect the output generated by the ADMT. The regulations also provide guidance about output types, and provide examples in § 7220(c)(5)(B) regarding information the business may include when disclosing to consumers the type of outputs generated by the ADMT and how that output is used for a significant decision. Further, § 7220(c)(5)(C) is clear that a business must disclose the alternative process for making a significant decision if a consumer opts out. These disclosure requirements are also consistent with similar requirements under other frameworks, such as the Colorado Privacy Act.
7220	435	Comment supports the ADMT pre-use notices being bundled with the existing Notice at Collection but urges further clarification. Comment argues that the Agency can avoid potential ambiguity that remains under the regulations concerning the pre-use notice requirements by further clarifying that the information required in a Pre-use Notice can be presented in a manner consistent with the existing CCPA requirements regarding Notice at Collection. Comment suggests that the Agency include illustrative examples	The Agency disagrees with this comment. The Pre-use Notice requirements are clear about how a business may consolidate this notice with a Notice at Collection. Specifically, a business may provide a Pre-use Notice in its Notice at Collection, provided that the Notice at Collection complies with, and includes the information required by, §§ 7220(b) and (c). The regulations are consistent and do not require illustrative examples. The comment's recommendation also appears to

		showing how businesses can present the Pre-use Notice as part of the Notice at Collection. Comment recommends an illustrative example as follows: "When a business uses ADMT as set forth in section 7200 and has posted a conspicuous link to its Notice at Collection on the introductory page of the business's website and on all webpages where personal information is collected, the business may provide a Pre-use Notice in its Notice at Collection."	misread the regulation, which explicitly requires compliance with §§ 7220(b) and (c).
7220, 7222	537	Comment criticizes the inclusion of trade secret exemptions in § 7220. The trade secret exemptions threaten to completely undercut the utility of the Pre-Use Notices and Right to Access—two of the most important provisions for consumers who want to understand how their data is being used to make major decisions about them. Comment suggests striking the trade secret exemptions from the Pre-Use Notice and Right to Access.	The Agency disagrees with this comment. Businesses must provide the required information in §§ 7220 and 7222. However, they are not required to provide trade secrets when providing that information. The regulations continue to ensure that consumers understand how an ADMT is used to make significant decisions about them, while providing protections for trade secrets.
7220(a)	303	Comment argues Pre-use Notice requirements should not apply to businesses only using ADMT with respect to personal data that is exempt under § 1798.145, e.g., GLBA, HIPAA, FCRA. It will likely lead to consumer confusion while imposing additional compliance burdens without benefits.	The Agency disagrees with this comment. The comment appears to misread the regulations. The regulations do not apply to information that is exempted from the CCPA. If a business is using ADMT to make a significant decision and no exemption applies, it must comply with the ADMT requirements in the regulations.
7220(a)	376	Comment suggests that allowing the Pre-use Notice to be provided in the larger Notice at Collection under certain circumstances is a practical and efficient approach. This consolidation reduces duplicative notice requirements and streamlines the regulations without diminishing transparency for consumers.	The Agency agrees with this comment and notes the comment's support.
7220(a)	418, 527	§ 7220(a) is ambiguous because it requires a Pre-use Notice for companies using ADMTs for exempt purposes that do not grant the right to access or opt out. Comment suggests that a Pre-use Notice should only be required when a business is required to offer an opt-out. Comment suggests adding "and	The Agency disagrees with this comment. The comment appears to misread the regulations. A business that is subject to an opt-out exception must still provide relevant disclosures in the Pre-use Notice, including, for example, the exception it is

		subject to the exceptions in section 7221(b)and section 7222(a)(1)," to the section.	relying on to not provide the opt-out or how to submit an appeal of a significant decision.
7220(c)	419	Commenter states support for the removal of the prohibition on justifying the use of decisions with terms like "to improve our services" to aid consumers in comprehension. Prohibiting the phrase is subjective and could preclude companies from using descriptions that are more easily understandable to consumers.	The Agency disagrees with this comment. The comment appears to misread the regulations. A business must not describe the purpose in generic terms. After receiving initial comments, the Agency revised the regulations to provide additional clarity on how a business must provide information in non-generic terms. The example clarifies that businesses must describe the specific significant decision being made with the ADMT. "Improving services" would never meet this requirement because this phrase does not describe a specific decision being made.
7220(c)(3)	304	Comment believes that access to ADMT would prove to be very problematic and harmful to both businesses and consumers.	The Agency disagrees with this comment. The CCPA requires the Agency to issue regulations governing opt-out and access rights regarding businesses' use of ADMT. (Civ. Code § 1798.185(a)(15).) Consumers have a right to access ADMT under the CCPA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Further, the access ADMT requirements balance providing privacy protections to consumers with flexibility for businesses to come into compliance.
7220(c)(5)	139, 167 316, 528, 564, 565	Comment appreciates the revisions to § 7220(c)(5), which represent a meaningful improvement by shifting away from requiring disclosure of ADMT "logic" and "key parameters" and instead focusing on how personal information is processed to make significant decisions. However, comment argues that requiring detailed descriptions of outputs and how they are used in Pre-Use Notices is excessive, may result in technical disclosures that offer little value to consumers, risk causing confusion, and may expose business logic unnecessarily. Comment also finds the requirements impractical given the complexity of many AI models. While the updated rules include the appropriate carveouts (§ 7200(d)), it still requires the notice to include a significant	The Agency agrees with this comment in part, to the extent that it supports the regulations. The Agency disagrees with this comment in part, to the extent that it recommends further modifications to the regulations. The Pre-use Notice requirements are not impractical and are analogous to similar requirements under the Colorado Privacy Act and the GDPR. In addition, the Pre-use Notice disclosures are necessary for consumers to have meaningful information about the use of ADMT so that they can exercise their CCPA rights to opt-out of ADMT and access ADMT. The regulations provide a flexible, performance-based standard for businesses regarding how to provide the required information. They also provide protections

		amount of information. Subsections (A) and (B) are problematic, and the Agency should carefully consider whether disclosure of this information outweighs any potential risks, and whether the risks would be better mitigated by robust internal assessment that requires rigorous testing. Comment recommends deleting Pre-use Notice entirely. If Pre-use Notice is required, it should be limited to manageable information. Specifically, comment suggests amending § 7220(c)(5)(A) as follows: "The categories of personal information processed by the ADMT," and striking § 7220(c)(5)(B).	for trade secrets. It is unclear how testing could replace the notice in ensuring that consumers receive this information.
7220(c)(5)	305	Comment urges deletion of this requirement, as it will require a business to distill complex AI models into a plain language explanation, which will likely result in the meaning of the explanation losing value. Additionally, even with the fraud prevention language found in §§ 7222(d), 7221, and 7222, this could provide a roadmap for fraudsters to target.	The Agency disagrees with this comment. The regulations require businesses to provide consumers with relevant information to exercise their CCPA rights to opt-out of ADMT and to access ADMT while providing flexibility to businesses in how to provide these notices. After receiving initial comments, the Agency revised the requirements to further simplify implementation for businesses at this time while still protecting consumers' privacy. Regarding the fraud prevention language, the comment does not explain how the Pre-use Notice requirements would provide a roadmap for fraudsters. The Agency believes the fraud prevention exception provides appropriate protections for businesses and consumers.
7220, 7222	143, 317, 426, 531, 532, 570, 571	Comment advocates limiting the Pre-use Notice and access right to cases in which the ADMT has made an adverse decision regarding the consumer. Comment also suggests including a Pre-Use Notice as a baseline disclosure, and then only upon an adverse decision could a consumer potentially obtain more individualized information. Comment recommends removing § 7222(b)(2)'s requirement to disclose methodology because it does not relate to privacy risks but does create a risk of requiring the disclosure of sensitive business information. Comment specifically recommends striking § 7222(b)(2) entirely because no other	The Agency disagrees with this comment. Comment's recommendation is less effective than the regulation at fulfilling the CCPA's mandate to ensure that responses to access requests includes meaningful information about the logic involved in the decisionmaking process, as well as a description of the likely outcome of the process, with respect to the consumer. Under comment's recommendation, consumers would receive less information about how decisions were made about them, which is less protective of consumer privacy. Further, § 7222(b)(2) implements the CCPA's requirement that responses to access requests include the logic of the decisionmaking

		regulatory frameworks that compel a business to explain an adverse decision require disclosing methodology, which has no correlation to any privacy risk to the consumer and could create a moral hazard. Requiring businesses to provide consumer-specific explanations even when no harm occurs goes beyond existing legal norms like Fair Credit Reporting Act ("FCRA") and the Equal Credit Opportunity Act ("ECOA"). Comment also states that § 7222(b)(3) is inconsistent with the definition of ADMT, because it implies coverage of interim tools rather than those that fully replace or substantially replace human decisionmaking and could make compliance impractical and undermine the efficiency of automated tools. The purpose of informing consumers is already addressed under § 7222(b)(1). In addition, comment recommends applying the same employment-related opt-out exceptions found in § 7221(b).	process. Similarly, § 7222(b)(3) implements the CCPA's requirement that responses to access requests include the outcome of the decisionmaking process for the consumer. They are consistent with the scope of ADMT and address a higher-risk use of ADMT to make significant decisions. The definitions of both ADMT and significant decision are also clear, and are both practical and flexible for businesses while addressing a higher-risk use of ADMT. These definitions and requirements are consistent with the CCPA and do not conflict with FCRA and ECOA. Further, the opt-out exceptions are intended to address circumstances where a business may not be able to offer an opt-out, and do not apply to the access ADMT context. The access ADMT requirements include relevant exceptions in § 7222(c). Additional exceptions are not necessary. With respect to sensitive business information, the regulations provide exceptions for certain trade secret and security, fraud prevention, and safety information.
7220(c), 7222(b)	534	Comment supports two revisions in §§ 7220(c)(5) and 7222(b)(3): requiring Pre-Use Notices to inform consumers how decisions will be made if they opt out, and requiring businesses to disclose outcomes of significant decisions in access requests.	The Agency notes comment's support.
7220(c)(5), 7222(b)(2)	167, 528, 565	Comment argues that there is ongoing ambiguity regarding the relationship between the disclosures required in § 7220(c)(5)(A) of the Pre-use Notice and those under the access right in § 7222(b)(2). § 7220(c)(5)(A) requires a plain-language explanation of how personal information is processed to make a decision, while the access provision requires disclosure of the ADMT logic. Without further clarification, the overlap between these requirements could create uncertainty about how much information must be disclosed in different contexts and increase the complexity of implementation. Comment recommends clarifying how	The Agency disagrees with this comment. The regulations are clear about how the Pre-use-Notice and access-ADMT requirements work together. A business must provide a Pre-use Notice at or before the point when it collects the consumer's personal information that it plans to process using ADMT. The Pre-Use Notice provides necessary information to the consumer so that they can exercise their CCPA opt-out of ADMT and access ADMT rights. If a consumer exercises their access ADMT right, the business must provide the information required in § 7222 so that a consumer understands the purpose for which the business used ADMT with respect to them, the logic of the ADMT, the outcome of the decisionmaking process for that

		these provisions interact to promote consistency and avoid duplication or conflict.	consumer, that the business is prohibited from retaliating against the consumer, and instructions regarding how the consumer can exercise other CCPA rights. Both §§ 7220(c)(5)(A) and 7222(b)(2) pertain to how the ADMT works. These requirements are consistent and do not create duplication or conflict.
7220(d), 7222(c)	43, 47, 97, 111	While supporting the trade secret and other exemptions added in § 7220(d), comment believes further protection of proprietary information is needed. Comment recommends that the Agency revise § 7220(d) to exempt all intellectual property and confidential business information and any information that a business would not generally make available to the public from inclusion in pre-use notices. Comment argues that the requirement for businesses to provide information about ADMT logic in § 7222(c) could result in the disclosure of intellectual property or confidential business information. Comment urges the Agency to exempt all intellectual property and confidential business information from inclusion in responses to access requests in § 7222(c).	The Agency disagrees with this comment. Additional exceptions are not necessary at this time, because the current exceptions already provide sufficient protections for certain trade secret, security, fraud prevention, and safety information. Further, commenter does not provide a standard of what would constitute confidential business information, which would render the comment's recommended exception unclear .
7220(d), 7222(c)	106, 375	Comment supports the narrowing of Pre-use Notice and consumer access request obligations to apply only to ADMTs used for significant decisions. It ensures that these obligations apply where potential impacts to consumers are most direct and avoids over-application to less impactful uses of ADMT where the risks are relatively lower. Comment urges the Agency to retain and refine this focused approach. Additionally, they support the provisions that protect trade secrets and security-related information from disclosure in Pre-use Notices and access responses, recommending keeping these protections and strengthening them.	The Agency notes comment's support. The regulations, both as proposed and revised, provide privacy protections for consumers and flexibility for businesses to come into compliance. After receiving initial comments, the Agency revised the ADMT requirements to further simplify implementation for businesses at this time while still protecting consumer privacy. With respect to strengthening the protections for trade secrets and other information, the Agency does not think that additional exceptions are necessary at this time. Current exceptions already provide sufficient protections for certain trade secret, security, fraud prevention, and safety information.
7220(d), 7222(c)	229	Comment contends that the fraud exemptions that the Agency retained for Pre-use Notice obligations and ADMT	The Agency disagrees with this comment. The regulations' exceptions balance providing information to consumers so that

		access rights remain too narrow. §§ 7220(d)(2) and 7222(c) fail to cover fraud prevention activities conducted by banking entities that are not "directed at" only the business or consumers.	they can meaningfully exercise their ADMT rights with flexibility for businesses and protections for certain fraud prevention information. Expanding this exception would not be more effective at protecting consumer privacy and would render the exception susceptible to abuse.
7220(d)(2)(B), 7222(c)(2)(B)	168	Comment argues that the language in §§ 7220(d)(2)(B) and 7222(c)(2)(B)—"resist malicious, deceptive, fraudulent, or illegal actions"—does not fully reflect the range of protective activities businesses engage in to secure systems and safeguard consumers. Narrowly framing the provision around "resistance" may exclude other critical functions such as prevention, detection, and investigation, which are essential components of a comprehensive security posture. Comment suggests expanding the exemption language to include prevention, detection, and investigation, to align with common cybersecurity frameworks and ensure operational integrity.	The Agency disagrees with this comment. The exception balances providing protections for businesses and protections for consumers to meaningfully exercise their ADMT rights. Comment's suggestion is no more effective or appropriate than the regulation adopted by the Agency.
7221	67	Comment supports the newly structured exceptions to the consumer's right to opt out of ADMT in certain important scenarios. Overall, these additions demonstrate the Agency's willingness to incorporate stakeholder input and craft exceptions that maintain consumer trust without inadvertently hampering security or beneficial uses of AI.	The Agency agrees with this comment and notes commenter's support.
7221	112	Comment argues that the regulations should clarify the scope of opt-outs to be implemented by service providers. The regulations allow consumers to opt out of ADMTs used when a business makes a significant decision. However, in some circumstances the regulations require a business to comply with a consumer's opt-out request by instructing all its service providers to remove a consumer from ADMT processing within a specified timeframe. This creates challenges because service providers do not generally have visibility into all the data they process on behalf of a	The Agency disagrees with this comment. The regulations are already clear that the opt-out to be implemented is "that ADMT" that the consumer has opted out of. This aligns with the fact that a business may engage in several uses of ADMT and may present a consumer with the choice to allow specific uses while also offering a single option to opt-out of all of the business's uses. (*See* § 7221(n).) In addition, the CCPA and existing regulations require service providers to know the personal information they process pursuant to their written contract with the business and the purpose for which they process it and require them to comply with all applicable

		business. Comment asks the Agency to clarify the scope of opt-outs to be implemented by service providers.	sections of the CCPA and regulations, including providing the same level of privacy protection for that personal information as required of businesses. (*See* §§ 7051(a)(2), (5).) The regulations add an example of a contractual requirement that a business may include in its contracts with service providers to assist the business in complying with its ADMT requirements. (*See* § 7051(a)(5).) The regulations are meant to be robust and applicable to many factual situations and across industries.
7221	461	Comment argues the opt-out right would restrict California businesses when developing their own productive ADMT applications internally by working off larger models from tech companies. It would also hinder efforts to address discriminatory outcomes, since opt-outs would lead to unrepresentative datasets and cause bias in automated decisions. This is even the case for those who do not opt out.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The regulations are consistent with the CCPA and provide consumers with a choice about whether they want to opt out of a business's use of ADMT, subject to certain exceptions. Respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations support the development of products and services that are both innovative and privacy protective. The regulations balance privacy protections for consumers and flexibility for businesses.
7221, 7001(b)	189	Comment suggests adding "and ADMT opt-out" link and § 7221 in § 7001(b).	The Agency disagrees with this comment. The Pre-use Notice must include the opt-out link for requests to opt-out of ADMT. The comment's recommendation would be less effective than the regulation, because it suggests that an opt-out link does not need to be included in the Pre-use Notice under § 7221(c)(1). A business must include an opt-out method with the Pre-use Notice to ensure that consumers can exercise their opt-out right when they are notified of a use of ADMT concerning them.
7221	194	ADMT opt-outs may not be practicable or safe in the medtech context and may interrupt patient care. Medtech providers may not know identity of patients' health-care-providers and may not be able to communicate opt-outs. Comment recommends exempting medical device manufacturers.	The Agency disagrees with this comment. The CCPA includes certain data-level exemptions for information governed by HIPAA, but it applies to "businesses" and is intended to supplement federal and state law. (*See* Civ. Code §§ 1798.140(d), 1798.145(c)(1), 1798.196.) The CCPA directs the Agency to issue regulations that govern access and opt-out

			rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA.
7221	264	Comment urges the Agency to reinstate requests to opt out of ADMT in § 7221. The Agency should reinstate the opt-out mechanism regardless of whether a human appeal option is offered.	The Agency disagrees with this comment. The regulations balance privacy protections for consumers and flexibility for businesses regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them. The Agency will continue to monitor the marketplace to determine whether modifications to the regulations are necessary.
7221	377	Comment strongly supports the removal of language that would have allowed a business to claim the opt-out exemption by relying on the ADMT developer's evaluation. This mechanism was unworkable given the distinct roles that entities hold in the AI value chain: while a developer can evaluate an ADMT for risks "in the lab," it has no visibility into, or control over, the ADMT once deployed "in the field." Additionally, it is the business, rather the developer, that uses the ADMT to make a significant decision and interacts directly with consumers.	The Agency agrees with this comment to the extent that it supports the Agency's regulations. To the extent the comment suggests that the regulations as initially proposed would have permitted a business to rely entirely upon an ADMT-developer's evaluation to meet its own obligations, the comment's interpretation of the regulation is inconsistent with the regulations' language. Previous §§ 7221(b)(3)(B)(i), (4)(B)(i), and (5)(B)(i) would have required the business to not only review the developer's evaluation of the ADMT, including any requirements or limitations relevant to the business's proposed use of the ADMT, but also to have implemented accuracy and nondiscrimination safeguards.
7221	538	Comment argues that removing consumer opt-out rights for first-party behavioral advertising conflicts with the CCPA's intent and statutory definitions of profiling. While first-party targeting should not be subject to a global opt-out as consumers are more likely to have varying preferences for personalization for individual companies, they still should have the ability to turn off personalization of offers if they so desire. Companies already offer individuals tools to manage first-party advertising as required by laws such as CAN-SPAM and the TCPA. The Agency should further require those	The Agency agrees with the comment to the extent that it supports protections for consumers' privacy. However, the Agency revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral advertising thresholds from Articles 10 and 11, to simplify implementation for businesses at this time. The regulations balance protecting consumers' privacy and simplifying implementation for businesses as this time.

		companies to let consumers turn off first-party ad behavioral profiling.	
7221(a)	566	Comment recommends deleting this section, as this is administratively difficult to implement without significant consumer benefit unless there is an adverse decision. If the right cannot be deleted, it should only apply as a right to appeal in the event of an adverse decision, like the Colorado AI Act and other similar laws. Comment suggests amending § 7221(a) to read as follows: In the event of an adverse significant decision having legal or similarly significant effect, a business must provide consumers with the ability to appeal the decision and in that appeal opt-out of the use of ADMT to make a significant decision concerning the consumer, except as set forth in subsection (b).	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The Agency modified the regulations to focus on a higher-risk use of ADMT at this time, which is a use without human involvement to make significant decisions. This balances protections for consumer privacy and simplifying implementation for businesses at this time. The comment's recommended amendments would be less clear and less effective than the regulations at protecting consumer privacy. Further, although the Agency strives for consistency with other privacy and laws when appropriate, it must comply with the CCPA and adopt requirements appropriate to California.
7221(b)	21	Comment argues that the revisions to the ADMT opt-out provisions further exacerbate the problem by removing the few barriers that existed to employers claiming the exemptions. As a result, an employer can simply pronounce that it is using a given ADMT solely for work allocation and assignment or compensation and that the ADMT does not discriminate.	The Agency disagrees with this comment. The regulations do not permit an employer to simply pronounce that it is complying with the regulations; a business must actually comply with the regulations. The opt-out exceptions balance providing privacy protections for consumers with flexibility for businesses, and simplify implementation for businesses at this time.
7221(b)	44	Comment states that the Agency outlines what businesses must do to qualify for the human appeal exception, including the designation of human reviewers that can review and analyze ADMT outputs, know how to interpret and use ADMT outputs, and have the authority to change related decisions. These requirements are overly restrictive and infringe on the operational prerogatives of affected businesses. Comment recommends the removal of these requirements.	The Agency disagrees with this comment. The requirements for qualifying for the human appeal exception are necessary to provide clarity to businesses on how to incorporate human review into their use of ADMT for significant decisions. It also provides a flexible, performance-based standard that is adaptable to a variety of use cases and contexts.

7221(b)	45	Comment repeats its assertion that the exceptions to ADMT opt-out rights should include situations where businesses aggregate and de-identify personal information once it is provided for automated decisionmaking. If such information cannot be reasonably associated or linked, directly or indirectly, with a specific consumer or household, it should qualify as an exception to the opt-out requirement. In addition, comment suggests that the Agency includes other exceptions similar to those available to personal information deletion rights in California Civil Code § 1798.105(d).	The Agency disagrees with this comment. The comment's recommendations are not necessary. To the extent a business is using aggregate consumer information or deidentified information as set forth in the CCPA, the CCPA already states that this is not personal information. (*See* Civ. Code § 1798.140(v)(3).) Personal information must identify, relate to, describe, be reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. (*See* Civ. Code § 1798.140(v)(1).) If information is not "personal information" as defined by the CCPA, it is not subject to the regulations' requirements. However, to the extent a business is using ADMT for a significant decision, it must comply with the regulations. Further, with respect to the deletion exceptions, it is unclear why those exceptions would be relevant to the use of ADMT for a significant decision. The opt-out exceptions in § 7221(b) are appropriately tailored to the use of ADMT for significant decisions, and additional exceptions are not necessary at this time.
7221(b)	71	Comment urges the Agency to provide greater clarity and flexibility around use-based exemptions, particularly when ADMT is embedded in multi-purpose systems. Under the modified draft, such a business could invoke the security/fraud opt-out exception only if the ADMT in question is used "solely" for those protective purposes. Comment is concerned that this strict interpretation might unintentionally penalize multi-use AI systems. Limiting the exemption to ADMT that is "necessary" and "solely" for security or fraud prevention could constrain the cybersecurity and anti-fraud capabilities of platforms that incorporate these functions into broader services. We recommend the Agency clarify that businesses can still qualify for the security/fraud exception even if the platform	The Agency disagrees with this comment. The regulations' requirements are reasonably clear, and they provide flexibility for businesses regarding how they ensure their compliance. The Agency believes that no further clarification is needed at this time. Regarding the security/fraud exception, the comment appears to refer to the proposed text published on November 22, 2024, not to the modified text of proposed regulations published on May 9, 2025. The modified text of proposed regulations published on May 9, 2025, reflects that the Agency removed the security, fraud prevention, and safety exception from § 7221(b) because it is no longer necessary in light of the other modifications the Agency has made to the regulations. Specifically, the Agency revised the definition of ADMT to focus on a higher-risk use of ADMT, which is a use without human involvement; and revised Article 11 to focus on the use of ADMT for significant decisions, to simplify implementation at

		or system has other functions, as long as the particular ADMT use at issue is for one of the protected purposes.	this time. The regulations balance privacy protections for consumers and simplifying implementation for businesses.
7221(b)	93	Comment argues that in the employment and hiring context, the ADMT opt-out right could result in dynamics that are unworkable and costly and would compel businesses to forgo the use of ADMT altogether. Comment argues that the exception set forth in § 7221(b)(1) that requires a business to allow an applicant/employee to appeal to a "qualified human reviewer" is the same as requiring them to opt-out completely from the use of ADMT in the first place.	The Agency disagrees with this comment. The opt-out of ADMT is not unworkable and does not pose unnecessary burden on businesses. Further, it is unclear how it would compel businesses to forgo the use of ADMT altogether. The opt-out right balances providing privacy protections for workers with flexibility for businesses to come into compliance. For example, the exception in § 7221(b)(1) addresses circumstances in which a business could not add human involvement at the time a decision is made but could provide a human appeal of that decision. Other exceptions explicitly address the employment context, such as hiring and allocation or assignment of work and compensation.
7221(b)	77, 170, 337, 422, 425, 441, 445, 510	Comment recommends reinstating the security, fraud prevention, and safety exception, arguing that it was critically important for systems designed to detect fraud, data breaches, or malicious activity. The current structure of the exceptions introduces limitations that could inadvertently restrict their application and increase compliance uncertainty. Requiring businesses to offer opt-outs for such systems compromises their efficacy, exposes consumers and companies to unnecessary risk, and provides little consumer privacy benefit. Reinstating the exception would protect consumers, public safety, and business integrity and help to harmonize with other privacy regulations on fraud prevention exemptions of opt-out rights. Comment argues that removing this exception could hinder rather than advance data security by creating opportunities for abuse by malicious actors and would conflict with federal law; comment notes that the Cybersecurity Information Sharing Act of 2015 ("CISA") guarantees private businesses the right to deploy defensive measures—including automated decisionmaking systems—	The Agency disagrees with this comment. The Agency removed the security, fraud prevention, and safety exception from § 7221(b) because it is no longer necessary in light of the other modifications the Agency has made to the regulations. Specifically, the Agency revised the definition of ADMT to focus on a higher-risk use of ADMT, which is a use without human involvement; and revised Article 11 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. The regulations balance privacy protections for consumers and simplifying implementation for businesses. It is unclear what the comment is referring to regarding harmonizing with other privacy regulations on fraud-prevention exemptions. The Agency strives for consistency with privacy laws in other jurisdictions when appropriate, but it must comply with California law and use its discretion to adopt requirements appropriate to California. The regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. It is unclear what the comment is referring to regarding

		to prevent security breaches and fraud. Comment suggests restoring and expanding the exception to provide consumers the ability to opt out of ADMT when the use of ADMT is necessary "to resist, prevent, and detect malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions," consistent with the language of ADMT Pre-use Notices (§ 7220(d)) and responses to requests to access ADMT (§ 7222(c)). Comment recommends explicitly confirming that processing carried out for fraud prevention and response purposes remains outside the scope of the opt-out right. Comment appreciates the narrowing of the scope of the ADMT requirements but calls for explicit exemptions for fraud detection and legal compliance activities, and specifically allowing the use of fraudsters' data for training ADMT models, which will help to prevent and catch future frauds. There should be a clear exemption for any legal and compliance-related activities which protect customers, investors, the firm, or the financial markets more broadly. Excluding such uses severely impedes the evolution of more efficient compliance systems which runs counter to the goals of the CCPA.	legal and compliance activities. The CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) The Agency does not believe additional exceptions are necessary at this time. Regarding the comment's suggestion about allowing the use of fraudsters' data to train ADMT models, the comment appears to refer to the proposed text published on November 22, 2024, not to the modified text of proposed regulations published on May 9, 2025. The modified text of proposed regulations published on May 9, 2025, reflects that the Agency removed the training threshold from Article 11 to simplify implementation for businesses at this time. The comment's suggestions are not more effective or appropriate than the Agency's regulations.
7221(b)	347	Comment suggests adding to the "opt-out" provisions a robust broad exception for processing that is necessary to perform a service requested by the consumer. The opt-out requirements pose a serious obstacle to functionality, and the exceptions in § 7221(b) are too narrow and contain requirements too disconnected from consumer privacy protection to fall under the Agency's mission or serve its purposes. Comment argues that although § 7221(b)(3) provides an exception from the opt-out requirements for when a business is using ADMT for task allocation, unfortunately, there is no opt out exception for promotion, demotion, suspension, and termination, and the exceptions	The Agency disagrees with this comment, because the uses of ADMT subject to Article 11's requirements are already limited to when the use of ADMT is for a significant decision. In addition, the comment's suggestion would limit consumers' right to opt out of ADMT in a way that would be inconsistent with the purpose and intent of the CCPA. Expanding or modifying the exceptions is not necessary. The current opt-out framework balances protections for consumer privacy and simplifying implementation for businesses at this time.

		remain too narrow, creating operation difficulties and unintended consequences that could harm consumers.	
7221(b)(2)	94	Comment appreciates the exception set forth in § 7221(b)(2), but argues that this exemption remains too narrow. In the employment context, the exemption also only applies for decisions related to the applicant's ability to perform at work and whether to hire them. In order for such an exemption to be useful in the employment context, it needs apply to all employment-related decisions and not be limited by terms that will result in needless litigation.	The Agency disagrees with this comment. This exception addresses the hiring context because it may not be feasible to provide consumers with the ability to opt-out of the use of ADMT for hiring, such as for same-day employment opportunities. It is not necessary to extend this exception to other types of employment decisions, because the same feasibility concerns are not present. For example, it is unlikely that a business is making so many termination decisions in a single day that an opt-out is unworkable. It is also unclear how this exception would result in litigation, and the comment does not explain how this would occur. The Agency does not believe that needless litigation will result.
7221	140, 170, 201, 271	Comment argues that § 7221's opt-out requirement is overly restrictive and sometimes infeasible given how ADMT is deployed. Opt-out should be tied to risk and feasibility. Comment asserts that the ability to opt-out of the use of ADMT to make significant decisions regarding the consumer and providing a method to appeal the decision for manual review by a human reviewer is very difficult to implement in the financial or lending space. Comment suggests that the word "solely" should be removed, and that low-risk uses of ADMT, such as to perform routine website maintenance should not trigger opt-outs. The current structure of the exceptions introduces limitations that could inadvertently restrict their application and increase compliance uncertainty. Comment urges clarification and expansion of exceptions for employment/education. Comment also suggests that "ensures" in §§ 7221(b)(2)(B), (3)(B) should be changed to "takes reasonable measures to ensure."	The Agency disagrees with this comment. The regulations require businesses to provide an opt out of ADMT where the business uses ADMT to make significant decisions about consumers without human involvement, which is a higher-risk use of ADMT. The regulations balance protections for consumer privacy and simplifying implementation for businesses at this time. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. Requiring that the ADMT be used "solely for" the purpose is necessary to protect consumers' right to opt-out of ADMT. Regarding the word "ensures," the comment appears to misread the regulations. §§ 7221(b)(2)(B) and (b)(3)(B) do not include the word "ensures."
7221(b)(2), (b)(3)	529	Comment argues that the language in § 7221(b) implies the exception to opt-out would not apply to ADMT used for assignment of work and business management of its	The Agency disagrees with this comment. It is unclear what the comment means by "business management of its products and services"; that phrase does not appear in the regulations.

		products and services, even though the latter is not a significant decision. Further, an ADMT deployer should be able to rely on an assessment or instructions from developer rather than be required to conduct an independent assessment. Comment suggests deleting "solely" in both §§ 7221(b)(2) and 7221(b)(3).	"Assignment of work" is a significant decision for consumers, but § 7221(b)(2) explains that a business does not need to provide an opt-out of ADMT when the business meets the criteria in that subsection. The requirements in §§ 7221(b)(2) and (3) that the ADMT be used "solely for" the purpose ensure that exceptions to the right to opt-out of ADMT are not overly broad. The performance-based standard in those subsections require that the ADMT work for the business's purpose and does not unlawfully discriminate based upon protected characteristics. This balances protections for consumer privacy and simplifying implementation for businesses at this time.
7221(b)(3)	113	Comment argues that the exceptions to the opt out rights should be revised to make them workable in practice. § 7221 should be revised, because it is unclear how a company would determine that the ADMT "works" for its purposes. Instead, comment recommends requiring a business to take reasonable steps to verify that the ADMT works for the business's purpose and to mitigate risks of unlawful discrimination based upon protected characteristics.	The Agency disagrees with this comment. Requiring that the ADMT "works for the business's purpose" and does not unlawfully discriminate based upon protected characteristics provides a flexible standard applicable to many factual situations and across industries. The comment's recommendation is not more effective or appropriate at providing clarity to businesses regarding how to determine that the ADMT works for the business's purposes and does not unlawfully discriminate. The regulations balance privacy protections for consumers and simplifying implementation for businesses at this time.
7221(b)(4)	568	Comment requests that the Agency remove the limiters "solely" in exceptions §§ 7221(b)(4) and (5)—so long as the ADMT is not used to make another type of significant decision, then the opt out should not apply. As written, it suggests that the exception would not apply to ADMT that is used for both assignment of work and how the business manages its products and services—even though the latter is not a significant decision. The standard "ensures" sets an unreasonably high bar. Comment proposes revising to say that a business must take reasonable measures to ensure. Also, an ADMT deployer should be able to rely on an	The Agency disagrees with this comment. In addition, it appears the comment refers to the proposed text published on November 22, 2024, not to the modified text of proposed regulations published on May 9, 2025. The modified text of proposed regulations published on May 9, 2025, reflects that the Agency revised Article 11 to focus on the use of ADMT for significant decision, and accordingly revised the exceptions to when a business must provide an opt-out from its use of ADMT. These revisions also include removing references to "work or educational profiling" from § 7221 and therefore removing § 7221(b)(5). With respect to the exception for allocation/assignment of work and compensation decisions in §

		assessment or instructions from developer rather than conduct an independent assessment.	7221(b)(3), previously § 7221(b)(4)(A), the Agency retained the requirement that the ADMT be used "solely for" the purpose to ensure exceptions to the right to opt-out of ADMT are not overly broad. The Agency also revised the regulations to include a performance-based standard that the ADMT work for the business's purpose and does not unlawfully discriminate based upon protected characteristics. This balances protections for consumer privacy and simplifying implementation for businesses at this time.
7221(c)	169, 233	Comment states that requiring multiple designated opt-out methods, as required by § 7221(c), adds operational burdens, particularly for digital-first businesses. Comment encourages the Agency to revise this provision to permit greater flexibility in how opt-out mechanisms are designed and presented, particularly for low-risk or high-value use cases. Comment suggests that the ADMT rules should more clearly recognize that businesses have flexibility to provide distinct opt-out experiences from different types of ADMT.	The Agency disagrees with this comment. The opt-out method requirements balance consumers receiving meaningful access to their right to opt-out of ADMT and flexibility for businesses in determining how to receive opt-out of ADMT requests. It is also consistent with similar requirements for other CCPA rights. (*See* §§ 7026(a), 7027(b).) This enables businesses to leverage their existing CCPA opt-out methods and extend them to the right to opt-out of ADMT, while ensuring that at least one of the methods for submitting requests reflects the manner in which the consumer interacts with the business. The regulations require businesses to provide an opt out of ADMT where the business uses ADMT to make significant decisions about consumers without human involvement. The Agency has determined that a business's use of ADMT to make significant decisions presents significant risk to consumers' privacy.
7221(f)	569	Comment requests to amend entire section to the following text only: A business may require a verifiable consumer request for a request to opt-out of ADMT set forth in subsection (a). A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information is subject to the business's use of ADMT.	The Agency disagrees with this comment. Requiring verification would limit consumers' right to opt-out of ADMT and be inconsistent with other CCPA opt-out rights. The inconsistency with other CCPA opt-out rights would limit businesses from leveraging their existing processes to meet ADMT opt-out requirements. (*See* §§ 7026(b)–(d), 7027(c)–(e).)
7221(g)	331	Comment opposes § 7221(g) requiring businesses to explain to consumers why a request was deemed fraudulent. They	The Agency disagrees with this comment. This requirement imposes a minimal burden on businesses while ensuring that businesses do not deny legitimate requests as potentially

		argue it could provide a roadmap for bad actors to infiltrate their systems.	fraudulent without giving the consumer the opportunity to learn of the reason for denial. The comment does not explain, and the Agency does not agree, that providing an explanation would provide a roadmap for bad actors to infiltrate their systems. The regulations do not require businesses to reveal their detection methods, and businesses have discretion in crafting the explanation. This requirement is also consistent with existing requirements of businesses and protections for consumers with respect to their exercise of other existing CCPA rights. (*See* §§ 7026(e), 7027(f).) This enables businesses to leverage existing processes for other CCPA rights and extend them to the right to opt-out of ADMT.
7221(i)	141, 169, 424, 530	Comment opposes a single opt-out. Comment raises concerns about the requirement for a single-user ADMT opt-out option because of the broad definitions of ADMTs, which could cause consumers to unknowingly opt-out of a broader set of tools than intended. Comment suggests that context-specific opt-outs will give consumers more autonomy and insight regarding the use of their data. Comment proposes use-case-specific opt-outs to avoid confusing consumers and suggests amending § 7221(i) as follows: In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of automated decisionmaking technology.	The Agency disagrees with this comment. Requiring a business to provide a single option to opt-out of all covered ADMT is necessary to prevent consumer confusion and to prevent businesses from presenting options to consumers in a strategic manner intended to curtail exercise of their right. It is also consistent with similar existing requirements for other CCPA rights (*see* §§ 7026(h), 7027(i)), which benefits businesses by enabling them to leverage existing processes for other CCPA rights and extend them to the opt-out of ADMT. The requirement does not prohibit a business from providing context-specific opt-out of ADMT information, as long as the business also offers a single option to opt out of all covered ADMT. The regulations balance privacy protections for consumers and flexibility for businesses regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them.
7221(n)(2)	381	Comment argues that the requirement for businesses to notify service providers to comply with the opt-out of ADMT request is unclear and potentially unworkable. Service providers lack the consumer relationship or technical access to implement opt-outs effectively. Comment recommends removing or clarifying this requirement to ensure it is	The Agency disagrees with this comment. § 7221(n)(2)'s requirement that a business notify other persons to whom it has made the consumer's personal information available using that ADMT that the consumer has opted out and instruct them to comply with the consumer's opt-out is necessary to protect consumers' right to opt-out of ADMT. This requirement is also

		workable in light of service providers' role in the ADMT value chain.	consistent with other CCPA opt-out rights. (*See* §§ 7022, 7026(f), 7027(g).) The regulations are reasonably clear, and the Agency believes that no further clarification is needed at this time.
7222	46	Comment suggests that the Agency should limit ADMT access rights to accessing personally identifiable information only. If the affected entity does not store the information in a manner that can be reasonably associated or linked, directly or indirectly, with a particular consumer or household, then it should not be subject to an access request. Such a change would ensure consistency with the right to access information in Civil Code § 1798.110, as well as general exceptions under §§ 1798.145 (j)(1) and (j)(3).	The Agency disagrees with this comment to the extent that it argues that the regulation is not clear. The regulations apply to the use of ADMT for a significant decision. The definition of ADMT already requires that the technology process personal information, so adding another provision regarding personal information is not necessary. The regulations for ADMT access rights are already consistent with the CCPA. Further, with respect to the exceptions under Civil Code § 1798.145(j)(1) and (j)(3), the Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. There is no requirement to reiterate these exemptions in the regulations, as doing so could create unnecessary complexity or confusion.
7222	74	Comment criticizes the explainability requirements as unreasonable and disconnected from the statutory privacy framework. Requiring businesses to provide detailed explanations about "parameters that generated the output" of an ADMT system—which can involve trillions of variables—is both infeasible and unhelpful to consumers. Instead of offering meaningful transparency, such mandates create confusion and compliance burdens while providing no measurable privacy benefit. We urge the Agency to refocus disclosures on actionable privacy protections and eliminate overly technical notice requirements.	The Agency disagrees with this comment. The CCPA requires that responses to requests to access ADMT include meaningful information about the logic involved in the decisionmaking process, as well as a description of the likely outcome of the process with respect to the consumer. (Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations implement these requirements and provide guidance regarding the types of information meet this requirement. The requirements are adaptable to a variety of use cases and contexts, and are not unduly burdensome. It is unclear how they would create confusion, nor does the comment provide examples or evidence that disclosure of this information would result in confusion. These requirements also benefit consumers by ensuring they have meaningful information about how an ADMT was used to make a significant decision about them.
7222	110	Information to be provided for access requests creates practical concerns. The regulations require businesses to	The Agency disagrees with this comment. The access ADMT requirements implement the CCPA's statutory direction that

		disclose to consumers information in response to access requests, including information about the logic used in the ADMT and how the business used the output of the ADMT to make a significant decision about the consumer, the business's plans to use the outputs of the ADMT to make an additional significant decision concerning the consumer in the future, and the extent of human involvement in future significant decisions. Such sensitive details may include competitive or other confidential information. Although the regulations include some protections for trade secrets, those provisions must be strengthened. Further, providing information about the logic behind individual consequential decisions may pose technical implementation challenges. Finally, comment suggests removing requirements to describe specific details of product improvements in response to access requests — both to avoid overly-long responses to consumers and to prevent disclosure of confidential information.	responses to access requests include meaningful information about the logic involved in the decisionmaking process and a description of the likely outcome of the process with respect to a consumer. Civ. Code § 1798.185(a)(15). They also balance ensuring that consumers receive meaningful information about how an ADMT was used to make a significant decision about them with flexibility for businesses to come into compliance, including providing exceptions for trade secrets and certain security, fraud prevention, and safety information. Further, commenter's recommendations would make the regulations less effective at ensuring consumers receive meaningful information about the logic involved in the decisionmaking process and a description of the likely outcome of the process with respect to a consumer, because consumers would not receive specific or necessary information about the use of ADMT.
7222	301	Comment supports the Agency's decision to exclude "training" uses of ADMT from Article 11.	The Agency notes commenter's support.
7222(a)	142, 171, 272, 427, 428	Comment believes that the CCPA does not mandate a separate notice to consumers. The Agency should implement a single set of rules about how businesses must provide meaningful information about their ADMT use. Businesses should be able to provide only high-level information in a notice rather than responses to specific requests. Consumer-specific responses are not required under the statute and go beyond the Agency's statutory authority. They run into over-disclosure issues and require details beyond the statutory mandate. Comment states the CCPA requires disclosure of only the overall "logic involved in the decisionmaking process" and the "outcome of the process" and does not require specific disclosures of logic or outputs. Comment also claims that the disclosure requirements are often	The Agency disagrees with this comment. The CCPA provides consumers with the right to access ADMT. The CCPA also explicitly requires that a business's response to access requests includes meaningful information about the logic involved in the decisionmaking process, as well as a description of the likely outcome of the process, with respect to the consumer. (*See* Civ. Code § 1798.185(a)(15).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. § 7222(a) is necessary to operationalize consumers' right to access ADMT, because a generalized notice or otherwise not requiring the disclosure of logic or the outcome with respect to the consumer

		impractical or infeasible, and do not provide significant consumer benefit for the cost of compliance. They can also be hard to answer without disclosing confidential information, which may harm consumers subject to "significant decisions" using ADMT. Consumers already have separate access rights under CCPA, allowing them to obtain any personal information companies process, including ADMT inputs and outputs containing their personal information. Furthermore, the exceptions for employment uses in § 7221(b) should also apply to this section. Comment also recommends narrowing access obligations to adverse decisions only. Further, if financial institutions are required to describe how a "significant decision" would be made without ADMT, then such institutions will face complexity outlining alternative manual processes that may not exist or be practical. Manual decision-making is inherently slower and more prone to human error, which results in inconsistent outcomes and undermines the efficiency and accuracy that ADMT may provide. Furthermore, explaining algorithmic processes in a way that is understandable to consumers would require significant effort and expertise, and may ultimately confuse the consumer. The requirement to disclose such detailed information could lead to frustration (especially with receiving another disclosure) and misinterpretation, potentially undermining consumer trust rather than enhancing it. Disclosing the logic of these algorithms could also compromise intellectual property and expose institutions to security risks. Moreover, revealing detailed information about the system could enable bad actors to better understand and potentially circumvent the institution's review processes, increasing the risk of fraud for all financial institutions. The right to access also overlaps with existing federal requirements under ECOA and FCRA.	would not meet the requirements of the CCPA. The Agency also revised the regulations to provide further clarity about what type of information may be provided to a consumer to meet the CCPA's requirements and to simplify implementation for businesses at this time. With respect to the comment's recommendation to apply the exceptions in § 7221(b) to the access ADMT requirements, it is unclear why this is necessary. Those exceptions address, for example, how to exercise a human appeal, and would not make sense in the access context, where the requirements address providing necessary information to a consumer to understand how an ADMT was used to make a significant decision about them. The regulations provide exceptions for trade secrets and certain security, fraud prevention, and safety information, which addresses comment's concerns about bad actors or compromise of business's information. Further, the CCPA provides exemptions for certain information subject to GLBA and FCRA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations apply only to personal information subject to the CCPA and do not conflict with other laws. Also, comment's recommendation would be less effective than the regulation at fulfilling the CCPA's mandate to ensure that responses to access requests include meaningful information about the logic involved in the decisionmaking process, as well as a description of the likely outcome of the process, with respect to the consumer. Under commenter's recommendation, consumers would receive less information about how decisions were made about them, which is less protective of consumer privacy.

7222(b)	307	Comment believes the potential costs to businesses of fulfilling these requests are likely to be significant and will impose substantial burdens on businesses to develop responses that meet the level of individualized explanation required by the regulation.	The Agency disagrees with this comment. The access ADMT requirements balance ensuring that consumers receive meaningful information about how an ADMT was used to make a significant decision about them with flexibility for businesses to come into compliance. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA and revised the regulations to further simplify implementation for businesses at this time. Those revisions include limiting the access requirements to the use of ADMT without human involvement, limiting the scope of significant decisions, simplifying the access response requirements, and providing additional time to come into compliance.
7222(b)	459	Comment argues that it is virtually impossible to provide access rights to ADMT training data on an individual level, as required by § 7222(b), because of how training data is combined. Explaining how a specific data point was used in training complex ADMT systems in "plain language" is also challenging and provides little privacy value to consumers.	The Agency disagrees with this comment. § 7222(b) provides a clear standard regarding providing consumers with information about the logic of the ADMT, which is required by the CCPA. It also provides guidance to businesses regarding the type of information that can be provided to consumers to meet this requirement. These are necessary to ensure consumers have meaningful information about how an ADMT was used to make a significant decision about them.
7222(b)(1)	421	Comment requests the removal of the prohibition on the phrase "to improve our services" when responding to consumers' requests to access ADMT. Comment states this improves consistency and consumer communications.	The Agency disagrees with this comment. A business must not describe the purpose in generic terms. "Improving services" would never meet this requirement because this phrase does not describe a specific decision being made.
7222(b)(2)	176, 380	Comment proposes revising access requirements that require disclosing parameters and specific outputs, as parameters vary across models and can be highly technical in nature and may be confusing or useful. Comment suggests reconsidering the inclusion of the parameters that generated the output and the specific output with respect to the consumer. Comment argues that the text retains explainability requirements focusing on highly technical aspects of ADMT tools, rather than on rights of access providing consumers meaningful information related to the	The Agency disagrees with this comment. The CCPA provides consumers with the right to access ADMT. The CCPA also explicitly requires that a business's response to access requests includes meaningful information about the logic involved in the decisionmaking process, as well as a description of the likely outcome of the process, with respect to the consumer. (*See* Civ. Code § 1798.185(a)(15).) The regulations provide further clarity about what type of information may be provided to a consumer to meet the CCPA's requirements. Parameters are provided as guidance for businesses about how to provide meaningful

		privacy of their personal information. The required information extends beyond the privacy access right authorized under the statute, and creates significant uncertainty for businesses while offering consumers no measurable privacy benefits. Providing consumers explanations of all the different parameters that have resulted in the output (assuming it is possible to even know this information, which is not always the case) is unlikely to provide the consumer with "meaningful information" as required by the statutory text. Creating further uncertainty for consumers and businesses, there is no consensus under the current state of explainability research on what information can or should be provided to explain how ADMT technology reaches a decision or how an output is generated. These practical challenges are likely to become even more pronounced as technology continues to evolve..	information about the logic of the ADMT. Similarly, how the business used the output to make a significant decision is necessary to provide consumers with meaningful information about the outcome of the decisionmaking process. Removing these provisions would make the regulations less clear and less effective at protecting consumers' privacy.
7222(b)(2), (b)(3)	144, 145	Comment believes that subsections (b)(2) and (b)(3) should be removed. Other regulatory frameworks, such as FCRA, that require businesses to explain decisions adverse to consumers do not require disclosing methodology. Requiring such disclosures provides no meaningful benefit to consumer privacy but does allow a backdoor means for competitors to access and copy a business's proprietary methodologies. Also, § 7222(b)(1) already covers cases where ADMT was the sole factor in the decision. If the decision was reached through a combination of automated outputs and human decisionmaking, it does not fall within the rules' definition of ADMT, which only applies where the technology substantially or fully replaces human decisionmaking.	The Agency disagrees with this comment. The CCPA provides consumers with the right to access ADMT. The CCPA also explicitly requires that a business's response to access requests includes meaningful information about the logic involved in the decisionmaking process, as well as a description of the likely outcome of the process, with respect to the consumer. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Not requiring the disclosure of logic or the outcome with respect to the consumer would not meet the requirements of the CCPA. Nevertheless, the Agency revised the regulations to provide further clarity about what type of information may be provided to a consumer to meet the CCPA's requirements and to simplify implementation for businesses at this time. Moreover, businesses are not required to disclose trade secrets when providing the information required for requests to access ADMT. With respect to § 7222(b)(1), the regulation is consistent with the definition of ADMT, and explicitly addresses a human's role in a decisionmaking process that does not meet the

			requirements for "human involvement." No further clarification is necessary.
Previous 7222(k)	352, 539	Comment urges the Agency to reinstate §§ 7222(k)(1)–(3), which requires businesses to notify individuals when they are subject to an adverse significant decision made using ADMT. These notice requirements promote accountability among system developers and deployers by creating a feedback loop incentivizing them to monitor for discriminatory outcomes and improve system fairness. The reminder notice also would have prompted consumers to consider their right to receive more information precisely when they would be most interested in using it.	The Agency disagrees with this comment to the extent that it recommends modifying the Agency's regulations but notes commenter's concerns. The regulations were revised to further simplify implementation for businesses at this time. They continue to balance providing privacy protections for consumers with flexibility for businesses to come into compliance.
Previous 7222(k)	378	Comment supports the removal of specific notice requirements for "adverse significant decisions" within the access section. These requirements previously created a parallel and duplicative notice regime within the access requirements, leading to unnecessary complexity.	The Agency notes commenter's support. The Agency disagrees with this comment to the extent that it suggests that the prior requirement was duplicative or complex. However, the Agency removed this requirement to further simplify implementation for businesses at this time.
Previous 7222(k)	572	Comment criticizes § 7222(k) for imposing burdensome requirements on businesses in the employment context by requiring detailed, individualized disclosures within strict timeframes for every "adverse significant decision."	The Agency disagrees with this comment. The comment appears to refer to the proposed text published on November 22, 2024, not to the modified text of proposed regulations published on May 9, 2025. The modified text of proposed regulations published on May 9, 2025, reflects that the Agency removed § 7222(k) to simplify implementation for businesses at this time.
ADMT	6	Comment asks whether a specific example regarding a fuel delivery company using AI to monitor truck driver routes, stops, and behavior, and then automatically flags them for further supervision review, would fall under the scope/definition of ADMT.	The Agency notes commenter's question. The definition of ADMT is clear and means any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking. Similarly, the use of ADMT must be for a significant decision to be subject to Article 11's access and opt-out requirements. Whether the use of AI to monitor truck drivers and flag them for supervision review is a use of ADMT for a significant decision

			would depend on whether the criteria for the use of ADMT are met by the specific facts surrounding the use.
ADMT	19	Comment argues that the changes to the definition of "significant decision" are detrimental. Comment raises concerns that the revisions exclude decisions about the "allocation or assignment of work" for independent contractors, when independent contractors are subject to data collection and algorithmic management. Similarly, the ADMT regulations no longer provide an opt-out for the use of worker data to train ADMTs. Lastly, the specific use of physical or biological identification or profiling to make significant decisions are no longer covered, even though these are error- and bias-prone systems.	The Agency disagrees with this comment. With respect to allocation or assignment of work, the Agency modified the regulations to limit this decision to employees to simplify implementation at this time. However, other decisions continue to apply to independent contractors, and provide protections for uses of ADMT for hiring, allocation/assignment of compensation, promotion, demotion, suspension, and termination. With respect to training ADMT for a significant decision, businesses must still conduct a risk assessment prior to doing so, which balances providing workers with privacy protections with flexibility for businesses to come into compliance. Further, physical or biological identification or profiling is still covered by the regulations. For example, the regulations require a risk assessment for certain uses. Similarly, consumers would have opt-out of ADMT and access ADMT rights to the extent a business was using it as ADMT to make a significant decision. Other CCPA protections, such as the right to limit and opt-out of sale/sharing, also continue to apply.
ADMT	20	Comment points out that the regulations eliminate the requirement for a use-notice when ADMT is involved in adverse decisions. This is a critical loss, since data access is the first step in Californians' ability to identify and challenge errors and unfair treatment. And even if a worker does request more information about a firing decision, for example, the current ADMT regulations no longer require the employer to share the actual output that was used in making that decision—rendering the ADMT access provisions a hollow promise.	The Agency disagrees with this comment. The adverse decision notice requirement was deleted to simplify implementation for businesses at this time. Workers continue to receive relevant notices under the regulations, including a Pre-use Notice to ensure they can exercise their opt-out and access rights. In addition, the access ADMT requirements ensure that workers receive meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to them; these requirements help to ensure that workers receive information about how an ADMT made a significant decision about them.
ADMT	40	Comment argues that Article 11 could improperly affect ADMT in vehicles and urges an exemption, asserting that the National Highway Traffic Safety Administration is the proper	The Agency disagrees with this comment. An exception for the use of ADMT in motor vehicles is not necessary, because the requirements only apply if a business is using ADMT for a

		regulator. Article 11 is overly broad and prescriptive. The Agency should specify that Article 11 does not apply to the use of ADMT in vehicles.	significant decision. An exception would also be less effective at protective consumer privacy. Further, Article 11's requirements are neither broad nor overly prescriptive. Rather, they provide clear requirements for businesses that are adaptable to a variety of use cases and contexts. The Agency also revised the regulations to provide additional clarity and guidance to businesses and further simplify implementation at this time.
ADMT	69	Comment urges the Agency to recognize within the regulations the distinct roles in the AI ecosystem, specifically the developers of AI models or software, the integrators who incorporate AI modules into larger systems, and the end-user deployers who actually use ADMT in practice. The current requirements are primarily written as if one entity is responsible for the entire ADMT lifecycle. In reality, compliance might be shared across multiple parties and this should be reflected in the regulations.	The Agency disagrees with this comment. The regulations' ADMT requirements apply to "businesses" and balance providing privacy protections to consumers with flexibility for businesses to come into compliance. To the extent an entity is a "business" and is using ADMT to make a significant decision about a consumer, that entity must comply with the ADMT requirements. The regulations also ensure that other relevant entities, such as businesses that make ADMT available to other businesses and service providers or contracts, provide facts or assistance as necessary to a business that must comply with these requirements. (*See, e.g.*, §§ 7050, 7153.)
ADMT	70	Comment recommends further tailoring the notice and opt-out provisions to avoid over burdening low-risk, routine uses of ADMT that are part of everyday operations. Comment suggests clarifying that Pre-use Notices and opt-out links are only required for ADMT uses that pose more than minimal risk to consumers or involve decisions of consequence.	The Agency disagrees with this comment. The Pre-use Notice and opt-out requirements apply to a business's use of ADMT without human involvement for a significant decision about a consumer. These are consequential decisions for consumers that are not low risk.
ADMT	81	Comment argues that the regulations sweep in a vast range of routine, low-risk business activities, such as automated systems that calculate small performance-based incentives or attendance-based bonuses. There is no identified privacy harm posed by such systems, yet they would be treated as if they represent the same kind of risk as unregulated AI tools with no human oversight. This disconnect reveals the underlying flaw in the Agency's approach: rather than targeting high-risk, high-impact use cases, the rules cast an unnecessarily wide net over ordinary business practices.	The Agency disagrees with this comment. The regulations are not overly broad. Automated tools such as those cited by commenter are subject to the ADMT requirements if they are used to make significant decisions without human involvement. This is a higher-risk use of ADMT that poses significant privacy risk, such as impairing consumer control over their personal information. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance.

ADMT	85	Comment argues that firms that provide ADMT-powered tools to small businesses would be forced to redesign their products to comply with the regulations, likely raising development costs. Those costs would almost certainly be passed on to small businesses.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance. Respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations foster the development of products and services that are both innovative and privacy protective.
ADMT	86	Comment believes that small businesses would face a catch-22 when considering new or continued use of ADMT that helps them navigate complex and ever-changing local, state, and federal regulations. Without automated tools, many small businesses will have more trouble managing compliance with various regulations. This could expose California small businesses to new risks and legal challenges.	The Agency disagrees with this comment. The regulations are consistent with existing law and enable businesses to leverage existing compliance processes to meet various requirements. In addition, the Agency revised the regulations to simplify implementation for businesses at this time, including small businesses. The comment does not explain how the regulations would expose small businesses to new risks and legal challenges. The Agency does not believe they will do so. Further, the regulations help reduce risks for businesses, such as security and privacy risks, and promote consumer trust and transparency.
ADMT	88	Comment expresses appreciation for prior revisions but remains concerned about the breadth of the regulations with respect to ADMT used for a significant decision and its potential impact on commercial credit reporting.	The Agency notes commenter's support. With respect to breadth, the Agency disagrees with this comment. The regulations are not overly broad but rather provide clarity about the businesses' obligations. With respect to impact on commercial credit reporting, the Agency also disagrees that the regulations will have a negative impact on this industry. The regulations balance providing protections for consumer privacy with flexibility for businesses to come into compliance.
ADMT	89, 90	Comment argues that while CCPA provides explicit exemptions, the regulations do not clarify how less fulsome exemptions that are specific to certain consumer rights in that statute would carry over to new ADMT. Without further	The Agency disagrees with this comment. The CCPA's statutory exemptions apply to the regulations. The Agency does not believe additional regulatory exceptions are necessary at this time. With respect to California businesses, the regulations do

		clarification, data vital to extending business credit arguably would need to be excluded from such systems or subject to a new ADMT opt-out. This interpretation could significantly disrupt established credit evaluation practices and create uncertainty for both businesses and service providers. Comment points out that failure to clearly extend the CCPA's commercial credit exception to the ADMT opt-out right could have a detrimental impact on California small businesses. Comment proposes adding language to explicitly exclude commercial credit reporting from the definition of "significant decision" in the ADMT rules. Proposed Amendment: (ddd)(7) A significant decision does not include the purposes set forth in 1798.145(o). This exemption would support the availability of credit to California businesses.	not impede access to credit. To the extent these businesses are subject to the regulations, the regulations ensure transparency when ADMT is used to make significant decisions without human involvement.
ADMT	91, 382	Comment acknowledges the Agency's attention and recent revisions but remains concerned that uncoordinated approaches to regulation of the same issue will result in competing, inconsistent and conflicting provisions that are difficult for businesses to implement. Comment argues that many of the same provisions of the ADMT regulations were considered by the Legislature last year in AB 2930 (Bauer-Kahan) and are being considered this year in a reintroduced measure, AB 1018 (Bauer-Kahan). Other pending legislative measures seek to regulate the use of ADMT in the employment context, including SB 7 (McNerney). Comment believes that any proper regulation of AI and ADMT in the employment context is the purview of the Legislature or the Civil Rights Department. To the extent that the Agency's regulation will apply to the employment context, the result will be competing, inconsistent and conflicting regulation of ADMT that will be nearly impossible for the business community to reconcile. Comment expresses concern about regulatory conflict between the ADMT rules and other existing or proposed California laws. Comment urges the Agency to prioritize harmonization with these concurrent	The Agency disagrees with this comment. Comment does not cite to any actual conflict with existing law. The regulations are consistent with both the CCPA and with existing law. With respect to legislative efforts, the Agency looks forward to continuing to work with stakeholders on future policy development.

		legislative and regulatory initiatives to ensure consistency and avoid a fragmented regulatory landscape that could meaningfully impact innovation without commensurate benefit for consumers.	
ADMT	114	Comment warns that California may soon have overlapping and conflicting AI rules from the Legislature, CPPA, and California Civil Rights Council ("CRC"). The Agency should work with its counterparts in the Legislature and at the CRC to help ensure consistency in proposed frameworks governing the use of automated tools. The Agency should also read its statutory mandate to issue regulations on ADMT narrowly, to decrease opportunities for potential conflicts in regulatory frameworks. The regulations appear to go beyond the CCPA's statutory mandate, in areas where other regulators and lawmakers are proposing and adopting policies.	The Agency disagrees with this comment. Comment does not cite to any actual conflict with existing laws or regulations. The regulations are consistent with the CCPA, with other privacy frameworks within the state and in other jurisdictions, and with other existing laws and regulations. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, the Agency is required to issue regulations and impose certain requirements. The regulations are not overly broad. Rather, they provide clarity and guidance to businesses about the scope of their obligations and flexibility for businesses to come into compliance. The Agency has engaged in robust preliminary rulemaking activities with a wide variety of stakeholders and looks forward to continuing to work with stakeholders, including the Legislature and other regulators, on future policy development.
ADMT	186	Comment argues that the text seeks to regulate areas that are preempted by federal law in violation of the supremacy clause or that conflict with federal law. The Defend Trade Secrets Act protects business trade secrets, which the Agency cannot abrogate. Nevertheless, the text requires a business to disclose business sensitive and trade secret-protected details, such as a plain language explanation of the "logic of the ADMT" for an ADMT access request. Additionally, the recognition that certain information need not be disclosed if it implicates a trade secret was not added to the section on ADMT opt-outs.	The Agency disagrees with this comment. The regulations do not conflict with federal law. The regulations also provide appropriate protections for trade secrets in the Pre-use Notice and access ADMT requirements. Comment also does not explain why a trade secret exception would be necessary to process an opt-out request, and the Agency does not identify a need to include one at this time.

ADMT	192	Comment supports the general direction of the ADMT regulations but argues that they would be overly burdensome to medical device manufacturers. Comment requests a clear exemption, especially when these manufacturers cannot determine the regulated status of the healthcare professional. This also ensures that the ADMT regulations do not pose unnecessary or harmful requirements on medical devices regulated by the FDA. Certain data processing activities involving health information are not covered by HIPAA and CMIA exemptions, and it would be inappropriate to subject such data processing to the ADMT regulations.	The Agency disagrees with this comment. The ADMT regulations are not overly broad or unduly burdensome. Rather, they balance providing privacy protections to consumers with flexibility for businesses to come into compliance. The Agency also revised the regulations to further simplify implementation for businesses. The CCPA also provides exemptions for certain medical information. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
ADMT	193	Comment urges the Agency to regulate health data uniformly and not have different privacy rules based on the type of entity in the health industry handling the same health data, such as for the opt-out of ADMT for significant decisions.	The Agency disagrees with this comment. The ADMT requirements, including the opt-out requirements, apply uniformly to businesses using ADMT for a significant decision concerning a consumer. The CCPA also provides exemptions for certain medical information. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
ADMT	195	Comment appreciates the Agency's revisions to the ADMT regulations but maintains that the latest draft still imposes overly broad and burdensome obligations on businesses, especially small and mid-sized employers.	The Agency disagrees with this comment. The ADMT regulations are neither overly broad nor unduly burdensome. Rather, they balance providing privacy protections to consumers with flexibility for businesses to come into compliance.
ADMT	198, 335, 340	Comment acknowledges improvements in the revision but notes that some concerns remain. The draft also creates a few new issues that raise potentially significant concerns that commenter urges the Agency to address.	The Agency disagrees with this comment to the extent that it suggests modifying the regulations. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance.
ADMT	205	Comment requests that the Agency include exemptions under Civil Code § 1798.145 in the ADMT regulations. In addition, comment urges the Agency to clarify that the commercial credit reporting exemption under § 1798.145 applies to ADMT-related opt-out rights.	The Agency disagrees with this comment. The CCPA's statutory exemptions apply to the regulations. With respect to California businesses, the regulations do not impede access to credit. To the extent these businesses are subject to the regulations, the regulations ensure transparency when ADMT is used to make significant decisions without human involvement.

ADMT	207, 416	Comment acknowledges improvements but argues that the ADMT regulations still contain fundamental flaws that could harm businesses, workers, and consumers in California. Article 11 is too broad and adds compliance burdens to low risk ADMT tools without clear privacy benefits to consumers.	The Agency disagrees with this comment. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance.
ADMT	209	California voters did not vote to police ADMT or scrutinize algorithmic task allocation. Comment shares Governor Newsom's concern about regulatory overreach impacting California's tech leadership. Comment believes that the Agency should withdraw the text, pending significant revisions.	The Agency disagrees with this comment. Voters, via the CPRA ballot initiative, specifically mandated that the Agency issue regulations governing access and opt-out rights with respect to a business' use of automated decisionmaking technology, including profiling. (*See* Civ. Code § 1798.185(a)(15).) This includes the use of ADMT for significant decisions, including significant employment decisions such as allocation or assignment of work. The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) These regulations are issued pursuant to the Agency's authority, are necessary to address the use of ADMT without human involvement to make a significant decision, which is a higher-risk use of ADMT, and balance providing privacy protections for consumers with flexibility for businesses to come into compliance. This approach fosters innovation in California.
ADMT	216	While comment supports transparency, it argues that Pre-use Notices and access rights must be tailored to significant decisions with real consumer impact to avoid user fatigue. § 7200(b) applies retroactively to tools no longer in use, and § 7220(a) appears to apply when no access or opt-out rights are triggered. Comment recommends limiting Pre-use Notice, access, and opt-out rights to consequential ADMT uses and high-risk use cases, and restricting access rights to adverse decisions. Comment also argues that the provisions that require explanation for the "logic" of complex ADMTs are not only impractical but risk confusing consumers and exposing proprietary information.	The Agency disagrees with this comment. The ADMT requirements are clear and tailored to significant decisions. With respect to § 7200(b), modifications are not necessary. It is not retroactive. A business using ADMT after the effective date of the regulations and prior to January 1, 2027, must be in compliance with Article 11's requirements for opt-out of ADMT and access ADMT rights no later than January 1, 2027. With respect to § 7220(a), the comment appears to misread the regulations. A business that is subject to an opt-out exception must still provide relevant disclosures in the Pre-use Notice, including, for example, the exception it is relying on to not provide the opt-out or how to submit an appeal of a significant

			decision. In addition, a business must always provide the information required in § 7222(b) in response to a request to access ADMT. However, it is not required to provide trade secret or certain security, safety, and fraud prevention information set forth in § 7222(c) when providing those disclosures. With respect to limiting access rights to adverse decisions, comment's recommendation is less effective than the regulation at fulfilling the CCPA's mandate to ensure that responses to access requests includes meaningful information about the logic involved in the decisionmaking process, as well as a description of the likely outcome of the process, with respect to the consumer. Under comment's recommendation, consumers would receive less information about how decisions were made about them, which is less protective of consumer privacy. With respect to disclosures of logic, the CCPA explicitly requires that a business's response to access requests includes meaningful information about the logic involved in the decisionmaking process, as well as a description of the likely outcome of the process, with respect to the consumer. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Further, the Agency revised the regulations to provide further clarity about what type of information may be provided to a consumer to meet the CCPA's requirements and to simplify implementation for businesses at this time. The requirements are not confusing but rather provide clear requirements that ensure consumers have meaningful information to exercise their ADMT rights. Moreover, businesses are not required to disclose trade secrets when providing the information required for requests to access ADMT. Comment also does not identify how the regulations fail to address consequential or high-risk uses of ADMT. The ADMT regulations address the use of ADMT for significant decisions, which ensures that consumers have meaningful transparency

			and control over their use of personal information for significant decisions in their lives.
ADMT	228	Comment supports refocusing the ADMT rules on tools that replace human decisionmaking but urges the Agency to further clarify the definition and provide more examples to avoid over breadth. Comment also raises concerns about the rules interfering with the fraud prevention and compliance activities of banks and their vendors, which may involve the processing of mixed data sets that include personal information that is not subject to GLBA. § 7221 removes entirely a partial fraud exception from the opt-out rights and creates risk for the consumers it seeks to protect by hobbling banks' ability to monitor for fraud.	The Agency disagrees with this comment. The definition of ADMT and the regulations are reasonably clear. The Agency believes that no further clarification or examples are needed at this time. Regarding information that is subject to GLBA, the CCPA's statutory exemptions apply to the regulations. The Agency removed the security, fraud prevention, and safety exception from § 7221(b) because it is no longer necessary in light of the other modifications the Agency has made to the regulations. Specifically, the Agency revised the definition of ADMT to focus on a higher-risk use of ADMT, which is a use without human involvement; and revised Article 11 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. A business can still deny opt-out of ADMT requests that are fraudulent. (§ 7221(g).) The regulations balance privacy protections for consumers and simplifying implementation for businesses at this time.
ADMT	230	Comment argues that it should be explicit that the new ADMT obligations do not compromise a business's ability to further compliance objectives, including identifying and preventing illegal activity. The Agency should not craft a more limited fraud exception to its new ADMT access rights than the fraud exceptions in the underlying statute for requests to know. Instead, it should be clear that businesses are not required to provide pre-use disclosures or ADMT access rights, and are not required to honor opt out rights, that would limit their ability to ensure "security and integrity" or to comply with laws, consistent with the underlying statutory framework.	The Agency disagrees with this comment. The CCPA's statutory exemptions apply to the regulations. Further, a business must comply with the Pre-use Notice and access ADMT requirements, but is not required to disclose certain trade secret, security, fraud prevention, and safety information when providing those disclosures to consumers. Similarly, a business must comply with the opt-out requirements unless an exception applies.
ADMT	259	Comment strongly supports the Agency's ADMT regulations and urges the Agency to uphold civil rights by adopting a comprehensive risk assessment framework based on the NIST AI Risk Management Framework.	The Agency notes commenter's support. With respect to the NIST AI Risk Management Framework, the regulations are consistent with other frameworks where possible while furthering the intent and purpose of the CCPA and providing

			clarity and guidance to businesses regarding their obligations. No additional modifications are necessary at this time.
ADMT	261	Comment urges the Agency to create a standardized incident reporting mechanism to identify problems or failures of ADMT systems. A standardized incident reporting system would enable the CPPA to collect consistent data on failures, biases, and harms across businesses utilizing ADMT. Having access to such data can allow the CPPA to identify recurring issues, for instance, if there is systemic bias in "significant decisions", for example, loan decisions applied across multiple financial institutions using ADMT—and separate isolated incidents from systemic vulnerabilities.	The Agency disagrees with this comment. Businesses must conduct risk assessments and submit relevant risk assessment information and reports to the Agency. These requirements comply with the directive to the Agency in the CCPA. The Agency does not believe an incident reporting mechanism is necessary at this time.
ADMT	282	Comment supports the Agency's decision to remove AI-related language from the rules. Regulatory frameworks at this stage are particularly vulnerable to misapplication and could lead to inconsistent enforcement or undue burdens on businesses. Introducing vague or overly broad AI-related requirements could have created significant compliance challenges without delivering meaningful consumer protections. By choosing to hold off on regulating AI at this time, the Agency has wisely preserved room for innovation.	The Agency notes commenter's support of the regulations. The ADMT requirements apply when a business uses ADMT to make a significant decision, regardless of whether the business used AI.
ADMT	285	Comment asserts that regulating AI tools that process personal data is within the CPPA's legal authority and essential to protecting privacy. The focus should be on how personal data is processed, not what tool processes it. Regulations also support innovation and create public trust and accountability.	The Agency agrees with comment, to the extent it supports the Agency's authority, the regulations, and their ability to foster innovation.
ADMT	318	Comment commends the Agency for revising the ADMT regulations by removing references to "artificial intelligence." Comment argues that AI is beyond the scope of the CCPA and the Agency's core competence. AI regulation is best left to other laws or legislative processes. Moving forward, the Agency must not attempt to regulate artificial intelligence as	The Agency notes commenter's support but otherwise disagrees with this comment. The regulations, both as proposed and revised, are within the Agency's authority. (*See* Civ. Code §§ 1798.185(a)(15), (b), 1798.199.40(b).) Nevertheless, the Agency has made efforts to limit the burden of the regulations while implementing the CCPA, including removing references to

		a technology. Instead, the Agency may only regulate artificial intelligence—and automated technologies more generally—to the extent they directly implicate consumer privacy.	artificial intelligence to further simplify implementation for businesses at this time.
ADMT	329, 330	Comment argues that Article 11's ADMT regulations duplicate other state rules and warns the Agency not to exceed its voter-approved mandate. Comment notes that multiple simultaneous regulations throughout the state pose significant challenges for the business community, creating unnecessary confusion and potentially conflicting rules. Therefore, comment states that no further actions should be taken regarding ADMT until the Agency has appropriately aligned with the Governor's and State Legislature's letters to the Agency. Comment also believes the regulations exceed the Agency's authority.	The Agency disagrees with this comment. The ADMT regulations are consistent with existing law. Commenter also fails to provide any examples of conflict or confusion with other state law. The Agency looks forward to continuing work with stakeholders on future policy development. Further, the ADMT regulations are within the Agency's authority. The CCPA directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment and submit it to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14).) The CCPA further directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (Civ. Code § 1798.185(a)(15).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements, including Article 10's risk assessment and Article 11's ADMT requirements when a business is using ADMT for a significant decision. The regulations are necessary to address the use of ADMT without human involvement to make a significant decision. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA.
ADMT	359	Comment argues that the expanded definition of ADMT in §7001(e) presents a timely and necessary regulation of algorithmic decision systems. However, the line between advanced analytics and regulated ADMT remains unclear, especially for small and medium size enterprises using off-the-shelf software or "low-code/no-code" automation tools. Comment urges the Agency to provide industry-specific	The Agency disagrees with this comment. The definition of ADMT is reasonably clear, and additional guidance is not necessary at this time. Further, businesses can leverage existing processes to comply with other CCPA notice and opt-out requirements to comply with the Pre-use Notice and opt-out requirements. Service providers and contractors must also comply with all applicable sections of the CCPA and these

		ADMT playbooks, with concrete examples and decision trees that help businesses assess whether their tools, configurations, or vendors fall under this regulation. Pre-use Notices and opt-out rights should also account for third-party platform use where configuration may not be fully under the business's control.	regulations. Additional modifications are not necessary at this time.
ADMT	383	Comment expresses support for the Agency's public engagement in the rulemaking process and the Board's emphasis on harmonizing the rules with other jurisdictions.	The Agency notes commenter's support.
ADMT	434	Comment strongly urges the Agency to adopt its regulations for businesses using ADMTs that would protect Californians' safety, privacy, and informed consent. These rules are a vital intervention for consumer protection and human rights as unaccountable algorithms increasingly influence our housing, education, employment, and basic freedoms. These rules should reflect the needs of everyday people to be protected from discrimination and data scraping, not Big Tech's appetite for profiting from personal information.	The Agency notes commenter's support.
ADMT	440	Comment argues that the regulations instead of targeting technologies like facial recognition or emotion detection, apply to low-risk functions like attendance tracking for bonuses or small incentive calculations, where there is no real privacy risk.	The Agency disagrees with this comment. The use of ADMT without human involvement for significant decisions, including for allocation or assignment of compensation, is not low-risk. These are consequential decisions for consumers that require a risk assessment and compliance with the ADMT Pre-use Notice, opt-out, and access requirements.
ADMT	460	Comment argues that imposing a backward-facing opt-out is unworkable when data has already been integrated into a model in a manner that does not permit reidentification. Deleting such data would require costly model reconstruction. Like the rule on data sales, this provision should be solely forward looking.	The Agency disagrees with this comment. The opt-out requirement is not unworkable. The regulations balance providing privacy protections to consumers with flexibility for businesses.
ADMT	478	Comment argues against leaving regulation of ADMT to Governor Newsom and the Legislature. Comment disagrees with lowering California's regulatory standards to align with	The Agency notes comment's support.

		weaker regimes elsewhere. Because California is home to many tech companies and major industry players, it is arguably in the best position to develop regulations that would affect its own resident businesses.	
ADMT	479	Comment rebuts the claim that training ADMTs should be excluded from regulation. Using personal information to train AI, when it was not collected for this specific purpose, contradicts California's constitutional right to privacy.	The Agency disagrees with this comment. The Agency removed training uses of ADMT from Article 11 to simplify implementation for businesses at this time. Further, a business must always comply with § 7002 when using consumers' personal information.

ARTICLES 9, 10, 11 – GENERAL COMMENTS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
CS Audits / RAs	310, 339	Comment argues that there is no precedent anywhere in the world for a government authority requiring individual attestation or executive sign-off for risk assessments or an annual cybersecurity audit. These sections should be amended so that third party auditors can work with internal audit and cybersecurity teams to conduct the cybersecurity audit for their objective expertise and ultimate collective sign-off. Comment argues that the requirement of an attestation under penalty of a perjury by a company executive in both the cybersecurity and risk assessment provisions (§§ 7124(d)(4) and 7157(b)(5)) should be removed. Requiring that cybersecurity audit reports or risk assessment be signed under penalty of perjury is excessive and incongruous with the contents and structure of those documents and will have the effect of weakening the purpose behind this requirement. Instead, comment recommends these provisions should be revised to require only a written submission by an individual familiar with and accountable for the cybersecurity audit or risk assessment	The Agency disagrees with this comment. For example, the New York Department of Financial Services requires covered entities to annually submit written certifications of compliance to the Superintendent that are "signed by the covered entity's highest-ranking executive and its CISO" or, if it does not have a CISO, by the "highest-ranking executive and by the senior officer responsible for the cybersecurity program of the covered entity." (N.Y. Comp. Codes R & Regs., tit. 23, § 500.17(b)(2).) The attestation requirement ensures accountability at the highest levels of the businesses. In addition, attestation under penalty of perjury is necessary to ensure that businesses submit truthful and accurate information to the Agency.

		process confirming that the audit or assessment was completed consistent with the regulations.	
RAs / ADMT	4, 101, 197, 308, 333, 441, 517, 566, 567	Comment recommends restoring the exemption in § 7221 allowing businesses to use ADMT for security, fraud prevention, or safety purposes without offering consumers an opt-out. Comment argues that such systems are essential for security, protecting consumers and confidential data, and protecting businesses from malicious activity. Subjecting uses of ADMT for these purposes to opt-out rights would reduce clarity, undermine their effectiveness, and compromise public safety. Comment argues that AI tools are important to identify and prevent zero-day attacks and malware-free attacks. Comment argues that removing the exception creates opportunities for abuse by malicious actors and would conflict with the Cybersecurity Information Sharing Act of 2015, which guarantees private businesses the right to deploy defensive measures—including automated decisionmaking systems—to prevent security breaches and fraud. Comment also argues that the removal of the exemption is contrary to the purpose of a similar exemption in § 7027(m). Comment recommends restoring the exception, updating the language for consistency with §§ 7220(d)(2) and 7222(c)(2), and adding "(D) To protect property or rights or defend against legal claims." Comment also recommends including the same "security, fraud prevention, and safety exception" in § 7150 as a new subsection (d), so that the full exemption applies to the requirements governing risk assessments for uses of ADMT for security, fraud prevention, or safety.	The Agency disagrees with this comment. The Agency deleted the exception in previous § 7221(b)(1) as unnecessary in light of the modifications the Agency made to the definitions of "ADMT" and "significant decision," and to the thresholds that trigger a business to comply with the ADMT requirements. (§§ 7001(e) and (ddd), 7200(a).) In modifying the regulations, the Agency considered the likelihood of a business using technology "without human involvement" to make a "significant decision" and determined that the regulations balance protections for consumers' privacy and preserving businesses' ability to protect themselves and consumers. (*See* §§ 7221(b)(2) and (g), which respectively address the human-appeal exception and permit a business to deny a consumer's opt-out request if the business believes it is fraudulent.) In addition, the CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) Regarding risk assessments, they ensure that businesses identify relevant risks and safeguards for processing that presents significant risk to consumers' privacy. This applies even if that processing activity is for security, fraud prevention, or safety purposes. For example, a business's use of ADMT to detect fraud can present significant risk to consumers' privacy, such as insufficient transparency, lack of control, and unlawful discrimination.
RAs / ADMT	5	Comment recommends continued engagement with stakeholders and emphasizes that any final regulation includes a mechanism for periodic revisions given the fast-evolving technologies.	The Agency agrees in part with this comment. The Agency looks forward to continuing to work with stakeholders on future policy development. The Agency disagrees in part with this comment. The regulations do not need to include a mechanism for periodic revisions, because the Agency can revise

			regulations as necessary, such as to adjust to technological changes.
RAs / ADMT	11, 12, 13, 15, 16, 273, 281, 348	Comment expresses concern about the scale back of the rulemaking on ADMT and risk assessment. They reflect significant concessions by the Agency and its board to a campaign of industry pressure and weaken consumer protections, including for communities of color. Comment advocates support for continuing the CPPA rulemaking process and opposes attempts to abandon or weaken it. They argue the Agency has democratic authority to make regulations and protect Californians from privacy harms. Comment warns that without strong protections, data collection and algorithmic systems can threaten consumer and worker rights. The efforts to derail the Agency's rulemaking is an "anti-democratic assault," that blocks the implementation of critical privacy rights for California's consumers and workers. Comment argues that AI is the scourge of society and used by technology companies to harness personal information for their own gain to the detriment of California citizens. Comment requests the Agency to remove the alterations and restore the original draft. Comment asks the Agency to support regulations that prevent AI and related technology from targeting Californians.	The Agency notes commenter's concerns. The regulations were revised to further simplify implementation for businesses at this time. The regulations continue to provide the strongest privacy protections for consumers, including workers, in the country. For example, they require businesses to conduct risk assessments for a variety of processing activities, including the use of ADMT for significant decisions and certain automated processing based on systematic observation of employees and independent contractors. They also provide necessary Pre-use Notices and access and opt-out rights for consumers with respect to the use of ADMT to make significant decisions about them. Additional modifications are not necessary at this time. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance.
RAs / ADMT	17, 277, 533	Comment expresses deep disappointment at the substantial weakening of the proposed regulations and notes that none of the recommendations provided by the commenter were adopted. They believe the current draft favors business interests and damages workers' and consumers' rights, and the ADMT and risk assessment regulations in their current form fail to meet the protective intent of the CCPA. Comment also argues that the revisions to the ADMT rules significantly weaken consumer protections by further reducing the number of businesses subject to the	The Agency notes commenter's concerns. The regulations as revised continue to balance providing privacy protections for consumers with flexibility for businesses to come into compliance. The Agency also disagrees with comment to the extent that it argues that the Agency is acting inconsistently with the CCPA's statutory delegation. The CCPA requires the Agency to issue regulations regarding cybersecurity audits, risk assessments, and ADMT. The Agency has issued regulations pursuant to that delegation to further the intent and purposes of the CCPA, including to provide meaningful control to

		requirements. The regulations roll back important transparency and accountability measures and undercut the purpose of the ADMT regulations and the CCPA itself. If adopted, the regulations will result in fewer Californians gaining insight into how their personal data is being processed in consequential decisions. Comment urges the Agency to undo the recent revisions and refocus on strengthening the proposed transparency measures for ADMTs to better protect consumers and increase trust in AI.	consumers with respect to their personal information. This includes requiring risk assessments for certain uses of ADMT and automated processing with respect to workers, and providing opt-out and access rights when businesses use ADMT to make significant decisions with respect to workers. The regulations ensure that the CCPA's statutory protections are operationalized with respect to all consumers, including workers.
RAs / ADMT	22, 23	Comment argues that the revised risk assessment provisions have become too weak for identifying and addressing ADMT harms. The regulations only serve to dilute the utility of risk assessments. For example, they no longer require businesses to: document whether they evaluated a given ADMT to ensure it works and does not discriminate; disclose the criteria they used to identify negative impacts to consumer privacy; and identify how their safeguards address any negative impacts identified in the risk assessment. Moreover, businesses no longer have to submit an abridged version of the risk assessment to the Agency. And perhaps most important, a critical provision in previous drafts, stating that businesses must not process personal information for use by an ADMT if the risks to consumers' privacy outweigh the benefits, was eliminated. The law requires, and Californians are entitled to expect, that risk assessments include the company's actual weighing of risks and benefits, and that the regulatory "goal" is "restricting or prohibiting" such processing if the specified risks outweigh the benefits. It is not enough to simply list various risks and benefits and assert that the risks are outweighed.	The Agency disagrees with this comment. The regulations are consistent with the CCPA. The Agency revised the risk assessment regulations to provide clarity to businesses regarding their obligations, and to further simplify implementation for businesses at this time while still protecting consumers' privacy. With respect to the examples cited by commenter, businesses must still conduct a risk assessment that identifies relevant negative impacts to consumers, including discrimination, and relevant safeguards. § 7154 has been revised to include the goal for risk assessments as indicated by the CCPA, which is restricting or prohibiting the processing of personal information when the risk to the consumer's privacy outweighs the benefits of the processing. With respect to submissions, businesses must still annually submit risk assessment information to the Agency and submit their risk assessment reports upon request.
RAs / ADMT	175, 302	Comment appreciates the Agency's decision to remove references to behavioral advertising and public profiling but believes that further revisions are necessary to avoid conflict with legal requirements and policy objectives of other	The Agency disagrees with this comment. Regarding training, the comment misinterprets the CCPA. The requirement to conduct risk assessments for certain training uses of personal information is within scope of the Agency's authority. The CCPA

		regulators and stretching the Agency beyond its regulatory remit. Specifically, comment argues that the Agency must remove training ADMT in order to avoid Agency overreach beyond the bounds of the statutory text as it does not constitute "use of" under the statute. The comment also recommends limiting ADMT to solely automated decisions and states that the statute requires this. These changes are also necessary to align with efforts by the governor and state Legislature. With respect to § 7200(b), comment also recommends the rule only apply when ADMT is the "sole basis" for significant decisions and to delay compliance until April 1, 2030.	explicitly states that the Agency must issue regulations requiring risk assessments for the processing of personal information that presents significant risk to consumers' privacy. (*See* Civ. Code § 1798.185(a)(14)(B).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) Training uses of personal information as set forth in the threshold present significant risk to consumers' privacy, such as data leakage that can reidentify consumers whose personal information was used to train the model and a lack of transparency and consumer control over the use of their personal information for training. Further, training is also a use of ADMT. § 7150(b)(6) is necessary because these training uses of ADMT present significant risks to consumers' privacy, and the regulations clarify when a business using personal information for training purposes must conduct a risk assessment. To the extent the comment suggests that the CCPA is limited to "solely automated decisions," the Agency disagrees. The CCPA's delegation to the Agency regarding ADMT is not limited to "solely" automated decisionmaking. Rather, the CCPA directs the Agency to issue regulations governing access and opt-out rights "with respect to a business' use of automated decisionmaking technology, including profiling." (*See* Civ. Code § 1798.185(a)(15).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) The ADMT regulations are within the Agency's authority, further the intent and purpose of the CCPA, and are necessary to address the use of ADMT without human involvement to make a significant decision, which is a higher-risk use of ADMT. These requirements are consistent with California law and align with efforts by Governor Newsom and the Legislature. The Agency has determined that delaying the implementation of these regulations any further is not more effective in carrying out the purpose and intent of the CCPA.

RAs / ADMT	185	Comment argues that several provisions potentially violate the First Amendment. Specifically, they include risk assessments, ADMT disclosures, ADMT pre-use notice, and businesses' response to an ADMT access right request.	The Agency disagrees with this comment. The Agency does not believe the requirements raise concerns under the First Amendment. Rather the regulations implement a valid state law.
RAs / ADMT	211, 258	Comment urges the Agency to explicitly clarify that exemptions under Civil Code § 1798.145 apply. Comment also specifically requests confirmation that the commercial credit reporting exemption under § 1798.145 applies in the context of ADMT-related opt-out rights. Comment supports additional clarity regarding the GLBA exemption to avoid confusion.	The Agency disagrees with this comment. The CCPA is reasonably clear in addressing which data are subject to the CCPA. The Agency believes that no further clarification is needed at this time.
RAs / ADMT	267	Comment urges the Agency to adopt targeted exemptions or phased implementation timelines for highly regulated sectors like real estate.	The Agency disagrees with this comment. The regulations are meant to be robust and applicable to many factual situations and across industries. They balance providing privacy protections to consumers with flexibility for businesses. The CCPA's statutory exemptions apply to the regulations. The Agency does not believe additional regulatory exceptions or additional phased implementation is necessary at this time.
RAs / ADMT	268	Comment argues that the regulations attempt to regulate information expressly exempt from the CCPA, such as personal information exempt under the GLBA and FCRA, in direct conflict with the Legislature's mandate in the CCPA. The Agency does not have authority to remove exemptions other than those necessary to implement the requirements imposed by the Legislature, which is not the case here.	The Agency disagrees with this comment, which appears to misinterpret the regulations. The CCPA includes data-level exemptions, including for information subject to GLBA and implementing regulations, and for the processing of personal information by certain entities, as long as the activity is regulated by the FCRA, and the processing is as authorized by the FCRA. (*See* Civ. Code §§ 1798.145(d), (e), 1798.196.) The CCPA's exemptions apply to the regulations. The regulations do not impose requirements on information that is subject to an exemption under the CCPA, such as the GLBA or FCRA exemptions.
RAs / ADMT	283	Comment supports the removal of "systematic observation" from the definition of "extensive profiling." Comment believes that this change brings clarity and relief to fuel retailers and convenience operators who rely on security and	The Agency notes commenter's support.

		surveillance systems to protect their customers, staff, and assets.	
RAs / ADMT	293	Comment argues that behavioral advertising and deepfakes should be identified as presenting negative privacy impacts. This helps clarify the harms and guide appropriate risk mitigation strategies.	The Agency notes commenter's concerns. However, the Agency revised the regulations to remove these provisions to further simplify implementation for businesses at this time. They continue to balance providing privacy protections for consumers with flexibility for businesses to come into compliance.
RAs / ADMT	477	Comment refutes the industry's claim that the Agency lacks authority to regulate ADMTs and risk assessments. The CCPA explicitly authorizes the Agency to promulgate regulations requiring companies to submit risk assessments to the Agency.	The Agency agrees with this comment and notes comment's support.
RAs / ADMT	508	Comment commends that the Agency added helpful language clarifying that Pre-use Notice requirements (§7220(d)) and responses to requests to access ADMT (§7222(c)) do not need to include trade secrets or information that would compromise a business's ability to combat fraud or prevent and address security, safety, and illegal behavior. Comment recommends the Agency to extend the same protections to risk assessments, such as the requirement to describe the "logic" of ADMT at § 7152(a)(3)(G) and disclosures to "recipient businesses" at § 7153(a). Additionally, the regulations should assure that the Agency will protect the confidentiality of materials submitted related to risk assessments.	The Agency disagrees with this comment. The exceptions are intended to address public disclosures of information to consumers. Extending these exceptions to the risk assessment requirements, which are internal-facing and submitted only to the Agency, is not necessary. Further, the CCPA already provides appropriate trade secret protections, and additional regulations are not necessary at this time. With respect to confidentiality, the risk assessment information and reports are only submitted to the Agency. With respect to the PRA, the Agency cannot amend the PRA or adopt regulations inconsistent with the PRA. Additionally, providing disclosures to the Agency does not equate to it being disclosed; whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the PRA applies.
RAs / ADMT	535	Comment argues that the revised definition of ADMT dramatically alters the scope of the regulations, excluding systems that are highly influential role in consequential decisions. The minimal human oversight is not a meaningful substitute for transparency, due to automation bias and	The Agency disagrees with this comment. To simplify implementation at this time, the Agency revised the definition of ADMT to focus on a higher-risk use of ADMT, which is a use without human involvement; revised Article 11 to focus on the use of ADMT for significant decisions; deleted § 7201; and

		company incentives to speed through review processes. These systems can be alarmingly off base, or can discriminate based on protected status. The April draft rules also had several provisions which might have prompted appropriate scrutiny, such as § 7201. The April draft also prohibited companies from processing data when the risks outweighed the benefits; that provision might have applied to these flawed systems, but it has now been weakened. Lastly, the information contained in the Pre-use Notice and request for access might have prompted Californians impacted by these flawed systems to reach out to the hiring entity or file a complaint with the Agency or the Attorney General. But such disclosures are no longer required if some human review is used, removing many of these checks.	revised § 7154 to clarify the goal of a risk assessment as stated in the statute. The regulations continue to provide the strongest privacy protections for consumers, including workers, in the country. For example, they require businesses to conduct risk assessments for a variety of processing activities, including the use of ADMT for significant decisions and certain automated processing based on systematic observation of employees and independent contractors. They also provide necessary Pre-use Notices and access and opt-out rights for consumers with respect to the use of ADMT to make significant decisions about them. Additional modifications are not necessary at this time. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance.
RAs / ADMT	541	Comment supports the Agency's overall direction, and notes improvements in narrowing ADMT obligations to high-risk scenarios and aligning risk assessment requirements with global norms, but urges the Agency to consider further narrowing its regulations (such as by removing training altogether and substantially paring back ADMT-specific access obligations).	The Agency notes commenter's support but otherwise disagrees with this comment. Training uses of personal information present significant risk to consumers' privacy and require a risk assessment. The access ADMT requirements implement the CCPA's statutory requirements and are necessary to ensure consumers receive meaningful information about how an ADMT was used to make a significant decision about them. More broadly, the regulations balance protecting consumer privacy and providing flexibility for businesses to come into compliance.
General	52, 79, 98, 174, 345, 442, 443, 464	Comment reiterates concerns about the ADMT, risk assessment, and cybersecurity audit rules, arguing they are overly broad, overstep the CPPA's statutory authority, and could impede legitimate business practices, including fraud detection. The regulations are misaligned with the Agency's core consumer privacy mission, and impose excessive burdens on businesses that far outweigh any potential consumer benefit. The Agency should allow companies that are subject to similar requirements in other states to leverage existing compliance efforts, to facilitate greater	The Agency disagrees with this comment. With respect to authority, the regulations are within the Agency's authority and further the intent and purpose of the CCPA, as amended by the California Privacy Rights Act, which California voters overwhelmingly supported via passage of Proposition 24 in 2020. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform a thorough and independent annual cybersecurity audit. (Civ. Code § 1798.185(a)(14).) The CCPA also directs the

		compliance and allow companies to focus on the core mission of all these regulations – better protecting consumer data. The Agency should continue to revise these rules to focus on the kinds of specific, meaningful privacy risks that motivated California voters to create the Agency, rather than creating sweeping requirements that would regulate and hamper a swath of routine business operations across California. The Agency should adopt a more targeted, risk-based approach that avoids stifling innovation. The current regulations would cause significant economic disruption without delivering commensurate benefits to privacy. The comment echoes calls from Governor Newsom and bipartisan legislators. Specifically, the Agency should: (1) narrow the rules to remain within the Agency's privacy mandate and (2) refrain from adopting requirements that would overburden innovation or impede the day-to-day operations of app-based platforms.	Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment and submit it to the Agency on a regular basis. (*Id*.) The CCPA further directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements. The regulations are necessary to operationalize the concepts introduced by the CCPA, and to provide clarity and specificity to implement the law. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. With respect to breadth, the regulations are not overly broad. Rather, they provide clarity and guidance to businesses about the scope of their obligations and flexibility for businesses to come into compliance. It is unclear how fraud detection would be impeded, because the regulations provide exceptions as necessary to address fraud prevention in the Pre-use Notice and access ADMT requirements. In addition, the reporting obligations are not onerous, and only require annual certification of completion of a cybersecurity audit and submission of risk assessment information to the Agency. Risk assessment reports must be provided upon request. With respect to existing compliance efforts, both the cybersecurity audit and risk assessment requirements explicitly enable businesses to leverage existing compliance processes.
General	14, 23	Comment strongly urges the Agency's board and the Agency to adhere to California's privacy law and continue with the rulemaking process as directed by the CCPA. Voters have been very clear that they want their information fully protected—and that includes future-proofing the CCPA by	The Agency disagrees with comment, to the extent that it argues that the Agency is acting inconsistently with the CCPA's statutory delegation. The CCPA requires the Agency to issue regulations regarding cybersecurity audits, risk assessments, and ADMT. The Agency has issued regulations pursuant to that

		developing regulations around cybersecurity, harm identification and mitigation, and algorithmic systems. What's at stake are highly consequential decisions impacting access and equity in our communities and our workplaces. Comment believes that the current drafting of the regulations falls short of the intent of voters and the directives of the CCPA itself. The regulations currently do not meet the broad goals of the CCPA, which are to ensure that consumers and workers have the information necessary "to exercise meaningful control" of businesses' use of their data and have "meaningful options" over how that data is collected, used, and disclosed. Comment suggests the Agency to complete its rulemaking by issuing rules that can form the foundation for an innovative, safe, and equitable future, free from undue influence and fully responding to the charge given by voters.	delegation to further the intent and purposes of the CCPA, including to provide meaningful information and control to consumers with respect to their personal information. This includes requiring risk assessments for certain uses of ADMT and automated processing with respect to workers, and providing opt-out and access rights when businesses use ADMT to make significant decisions with respect to workers. The regulations ensure that the CCPA's statutory protections are operationalized with respect to all consumers, including workers.
General	183	Comment raises concern that the regulations "risk creating a fractured regulatory landscape" and placing "less resourced companies at a competitive disadvantage." Comment urges aligning the regulations to other U.S. state privacy frameworks as harmonizing the requirements with other state privacy laws is consistent with the CCPA statute's intended goals and the APA. Comment recommends that risk assessment requirements conform to those in the Colorado Privacy Act regulations and should recognize that risk assessments completed under frameworks with "reasonably similar scope and effect" satisfy the CCPA. Comment also recommends deleting the attestation requirement that the business has not attempted to influence the auditor's decisions or assessments and permitting businesses to conduct a full cybersecurity audit every three years with annual "intervening" audits. Comment also recommends revising ADMT definition to limit it to "solely automated significant decisions," to avoid a "complex patchwork of state regulations" that "discourage[s] entrepreneurialism."	The Agency disagrees with this comment. Regarding regulatory burdens, the majority of the costs of the regulations fall on larger businesses dealing with large amount of personal information and with annual revenues that are greater than $28 million. The Agency has made efforts to limit the burdens of the regulations while implementing the CCPA. Regarding aligning regulatory requirements with other jurisdictions, although the Agency strives for consistency with privacy laws in other jurisdictions when appropriate, it must comply with California law and use its discretion to adopt requirements appropriate to California. Regarding other risk assessment frameworks, § 7156(b) is clear that businesses can leverage existing compliance processes while meeting the CCPA's requirements for a risk assessment. The Agency disagrees with the comment's recommendation to delete the attestation that the business has not attempted to influence the auditor, because the requirement is necessary to preserve the independence of the auditor's decisions and assessments; it addresses the risks that businesses will seek to influence auditors' assessments of their

		Comment also recommends amending regulations to recognize that risk assessments and cyber audits do not weaken claims of attorney-client privilege or work product protection and are protected from public disclosure.	cybersecurity posture. The Agency disagrees with the comment's recommendation to permit businesses to complete cybersecurity audits once every three years, because that would be inconsistent with the CCPA, which requires the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to "perform a cybersecurity audit on an annual basis." (Civ. Code § 1798.185(a)(14)(A).) Regarding the definition of ADMT, the CCPA's delegation to the Agency regarding ADMT is not limited to "solely" automated decisionmaking. Rather, the CCPA directs the Agency to issue regulations governing access and opt-out rights "with respect to a business' use of automated decisionmaking technology, including profiling." (*See* Civ. Code § 1798.185(a)(15).) The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) Further, regarding public disclosure or submission of privileged information, neither the cybersecurity audit nor risk assessment regulations require submission of privileged information. The cybersecurity audit regulations require a business to submit a certification of completion to the Agency, not its cybersecurity audit report. (*See* § 7124.) With respect to the PRA, the Agency cannot amend the PRA or adopt regulations inconsistent with the PRA. a statute by regulation. Additionally, providing disclosures to the Agency does not equate to it being disclosed; whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the PRA applies.
General	244, 245, 444	Comment urges the Agency to create exemptions from the three new areas of rules for financial institutions, including broker-dealers, registered investment advisers, and banking organizations, as well as their holding companies and affiliates. These institutions already comply with overlapping	The Agency disagrees with this comment. Exempting financial institutions would be inconsistent with the CCPA, which instead includes a data-level exemption for information subject to the GLBA and implementing regulations; it applies "businesses" and does not exempt financial institutions. (*See* Civ. Code §§

		and rigorous federal regulations under laws like GLBA and frameworks from the SEC, FINRA, and others. The regulations would impose redundant and burdensome obligations that divert resources from existing protections. This will avoid conflict with these organizations' federal regulation and supervision and prevent unintended and detrimental impacts on the safety and soundness of the U.S. banking and payments systems. This avoids issues of legal preemption and exclusive visitorial rights for the OCC over national banks and federal savings associations. Comment says cybersecurity audits and risk assessment regulations as currently drafted would interfere with OCC's visitorial rights. In addition, the rules would interfere with the authority that banks and savings associations have to use technology to deliver banking products and services. Comment states that there are strong policy rationales for adopting exemptions for banking organizations, because federal regulators already supervise cybersecurity and risk assessment practices and the use of ADMT by banking organizations and their affiliates. Comment states that imposing duplicative requirements in the rules would divert resources from promoting privacy and safeguarding the banking system in accordance with existing federal frameworks without corresponding benefit.	1798.140(d), 1798.145(e).) In addition, the CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) The CCPA directs the Agency to issue regulations that require businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform an annual cybersecurity audit, and establish a process to ensure that audits are thorough and independent. (*See* Civ. Code § 1798.185(a)(14)(A).) The CCPA also directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment, and requires that risk assessments be submitted to the Agency on a regular basis. (*See* Civ. Code § 1798.185(a)(14)(B).) The CCPA also directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations already provide flexibility for businesses. § 7123(f) enables a business to utilize cybersecurity assessment work it has already done, provided that it meets all of the Article 9 requirements, either on its own or through supplementation; and § 7156(b) enables businesses to leverage existing compliance processes while meeting the CCPA's requirements for a risk assessment.
General	246	Comment appreciates the Agency's efforts and the improvements in the regulations but believes the regulations still raise several serious concerns for the banking sector, particularly due to its overlap with established federal regulatory systems and the operational risks introduced by certain prescriptive state-level mandates.	The Agency disagrees with this comment. The regulations are consistent with federal and state laws. In addition, the CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) Further, it is unclear what operational risks the comment is

			referring to. However, the Agency disagrees that the regulations would introduce such risks. They provide clear and flexible standards and appropriate protections for consumers and businesses.
General	482	Comment refutes the industry argument that privacy regulation stifles innovation. Innovation without proper safeguards is reckless. This privacy-protective, thoughtful progress is the type of innovation that regulations like the Agency's November 2024 proposal should and do incentivize.	The Agency agrees with this comment and notes comment's support. The Agency revised the November 2024 regulations to further simplify implementation for businesses at this time while continuing to provide the strongest privacy protections for consumers, including workers, in the country.

ARTICLE 12. INSURANCE COMPANIES

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7271(a)	25	Comment requests to preserve consistency and avoid any ambiguity between the illustrative examples and § 7271(a). § 7271(a) should be revised to add "or that is otherwise exempt under California Civil Code Section 1798.145." And the second sentence with the example should be deleted.	The Agency disagrees with this comment. The regulation is reasonably clear and the examples provided adequately explain what is meant by personal information that is subject to the Insurance Code. The suggested clarification is unnecessary as Civil Code § 1798.145 already provides exemptions for personal information subject to the Gramm-Leach-Bliley Act ("GLBA") and California Financial Information Privacy Act ("CFIPA"). The comment does not provide a reason why the second sentence should be removed. The Agency believes it is necessary to clarify what is meant by personal information subject to the Insurance Code.
7271(b)(3)	24	While the comment appreciates the intent to clarify the boundaries of the CCPA's applicability to insurance data in § 7271(b)(3), comment is concerned that the example continues to reflect a misunderstanding of the data level exemptions in Civil Code §§ 1798.145(c), (d)(1), and (e). Specifically, in illustrative example § 7271(b)(3), the revised language describes a scenario in which a consumer ("Sloane") submits personal information as part of a claim for fire	The Agency disagrees with this comment. The Agency has added the counterexample to demonstrate an instance where information covered by the Insurance Code is not subject to the CCPA. The suggested clarification is unnecessary as Civil Code § 1798.145 already provides exemptions for personal information subject to the GLBA and CFIPA.

		damage. The Agency concludes that this information is "used to service the insurance policy" and thus "not subject to the CCPA." Comment agrees with the conclusion but believes the rationale must be more clearly anchored in the CCPA's statutory exemption for GLBA data. Therefore, comment requests that the example be revised to read: "(3) Sloane submits personal information to her insurance company as part of a claim for losses incurred by a fire at her home. This information is used to service the insurance policy, and thus subject to the Gramm-Leach-Bliley Act, the California Financial Information Privacy Act, and the Insurance Code and its regulations. This nonpublic personal information is not subject to the CCPA."	
7271(b)(3)	49	Comment criticizes the third illustrative example for being unclear and inconsistent with the CCPA. Comment argues the example conflates the status of data as subject to the GLBA with the purpose for which it is being processed. It also does not address the fundamental concern that the insurance regulations risk exacerbating complexity and resulting consumer and industry uncertainty, without any material improvement for privacy. Comment reiterates the prior comments and suggestions for edits to the regulations.	The Agency disagrees with this comment. Civil Code § 1798.185(a)(20) requires the Agency to adopt regulations applying the parts of the CCPA that are more privacy protective than the Insurance Code to insurance companies. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. These regulations are necessary to address any ambiguity regarding insurance companies' obligations under the CCPA and do not introduce new laws, nor amend existing legal rights or requirements. The example is consistent with the CCPA's statutory exemptions, which exclude personal information collected, used, processed, or retained by insurance companies pursuant to specified federal and state laws, including the Insurance Code and GLBA. The example clarifies that personal information submitted "as part of a claim for losses incurred by a fire" is used in connection with servicing an insurance policy, an activity that falls within the scope of an insurance transaction as defined in Insurance Code § 791.02 and is therefore exempt from the CCPA. Further, the example does not conflate legal standards but rather clarifies that personal information collected in connection with the servicing of an insurance claim is regulated under the

			Insurance Code exempt from the CCPA. Comment seems to misconstrue the plain language of the regulations.
Insurance	26, 50, 51, 199	Comment highlights ongoing legislative efforts, such as SB 354, to update California's insurance privacy law (IIPPA). They argue that if enacted, SB 354 would substantially update insurer data practices and potentially render Article 12 unnecessary. A potential NAIC model law would also make it premature for CPPA to proceed. Conflicting regulatory regimes would increase compliance burdens and consumer confusion. Moving forward now means the Agency would likely need to commence a new rulemaking process later anyway to cure the unnecessary complexity. They recommend deferring action on Article 12 until SB 354 is resolved or clear authority is clarified, particularly given the pending legislation (SB 354) and existing Department of Insurance oversight. Comment also recommends the Agency add explicit language that the likelihood of successor legislation will enhance and further clarify current law to defer to successor legislation where conflicts may arise.	The Agency disagrees with this comment. Civil Code § 1798.185(a)(20) requires the Agency to adopt regulations applying the parts of the CCPA that are more privacy protective than the Insurance Code to insurance companies. The CCPA also grants the Agency the authority to adopt additional regulations as necessary to further the purposes of the CCPA. (*See* Civ. Code §§ 1798.185(b), 1798.199.40(b).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. These regulations are necessary to address any ambiguity regarding insurance companies' obligations under the CCPA. These regulations also acknowledge that the CCPA and Insurance Code may overlap in their jurisdiction and delineate the boundary between the two legal frameworks. Moreover, comment's suggestion of referring to successor legislation does not comply with the APA's clarity standards.
Insurance	48	Comment urges the Agency not to adopt the insurance-related regulations at this time, arguing that doing so could confuse consumers and add complexity without providing privacy protections.	The Agency disagrees with this comment. Civil Code § 1798.185(a)(20) requires the Agency to adopt regulations applying the parts of the CCPA that are more privacy protective than the Insurance Code to insurance companies. These regulations are necessary to address any ambiguity regarding insurance companies' obligations under the CCPA. They do not introduce new laws, nor amend existing legal rights or requirements. These regulations acknowledge that the CCPA and Insurance Code may overlap in their jurisdiction and delineates the boundary between the two legal frameworks.

OTHER TOPICS – COSTS AND GENERAL

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
Costs	78, 84, 87, 99, 184, 217, 265, 384, 438	Comment appreciates the Agency's effort to lower compliance costs but notes the burden remains high, especially for small and medium-sized businesses. The compliance costs of the regulations are projected to reach over $1.2 billion in the first year. Comment acknowledges that while definitions have improved, the structure and burden of the regulations remain problematic. The regulations are overly expansive and substantial financial and operational burdens that will impact businesses and housing and lending participants without meaningfully improving consumer privacy. Comment warns that the economic cost of compliance is excessive and beyond what is estimated in the SRIA. Comment warns this would divert resources away from job creation and innovation. Comment urges the Agency to more carefully consider the impact and costs of the regulations on small businesses and the state, and strive for balanced regulations that reduce —rather than increase —barriers to California small businesses' success." The Agency should update the SRIA to ensure that the actual cost of the text is fully understood to allow the Board to assess whether the right balance has been struck across the range of available alternatives for the regulatory text. Comment urges the Agency to continue refining the economic impact analysis and consider phased implementation timelines, size-based thresholds, or alternative compliance paths that preserve the rules' objectives while mitigating the unintended consequence of discouraging competition and job growth.	The Agency disagrees with this comment. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance. The Agency has revised its Form 399 to reflect the updated economic analysis. The Agency's modifications to the regulations, which include phased implementation and size-based thresholds, significantly reduced the costs on all businesses, including for small businesses, from $9.725 billion to $4.835 billion over 10 years. The number of jobs lost in the first year also decreased, and the number of jobs created over 10 years increased to 348,000. The gross state product in the 10th year also increased from to $369 billion. Moreover, the regulations generate significant benefits for businesses and consumers, which are net positive one year after implementation and total $277 billion over a 10-year period; these benefits only reflect quantifiable benefits resulting from avoided business cybersecurity financial losses. There are many other benefits that cannot be quantified at this time. Overall, the regulations strike the right balance between costs and benefits; indeed, the benefits greatly outweigh the direct costs associated with them.
Costs	266	Comment argues that the audit, risk assessment, and ADMT requirements impose financial burdens that could ultimately harm consumers by reducing housing affordability and mortgage approvals, especially for vulnerable populations like first-time and first-generation buyers.	The Agency disagrees with this comment. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance. For example, with respect to the use of ADMT to make significant housing decisions, businesses can leverage existing compliance processes to conduct its risk

			assessments, such as similar assessments done to comply with analogous requirements under Colorado law or GDPR. With respect to the Pre-use Notice, opt-out and access requirements, the Agency revised the requirements to simplify implementation at this time, including limiting the requirements to the use of ADMT without human involvement, streamlining disclosure requirements, and providing businesses additional time to come into compliance.
Costs	322	Comment warns that although the rules strike direct references to AI, it is very likely that AI systems will continue to be regulated under the definition of ADMT. For this reason, comment believes that the cost of implementing ADMT rules will be much higher than the $143 million cited by the Agency.	The Agency disagrees with this comment. The cost evaluation focuses on the use of the technology and not on whether it is AI. The ADMT requirements apply when a business uses ADMT to make a significant decision, regardless of whether the business used AI. Modifying the definition of ADMT to focus on technology that replaces or substantially replaces human decisionmaking, and requiring businesses to comply with ADMT requirements only when they use ADMT to make a significant decision concerning a consumer, significantly reduced the number of businesses the Agency estimates are subject to the rules. Based on the Agency's knowledge and expertise regarding how businesses use ADMT to make decisions, the Agency estimates that 10% of businesses will be required to comply with the ADMT rules. The Agency made a good faith effort to estimate the costs associated with these regulations. The comment provides no specific data that would undermine the Agency's economic analysis.
Costs	361	Comment argues that the CCPA regulations are deeply legalistic, and many small and medium size enterprises cannot afford to hire privacy counsel or in-house compliance leads. Without accessible self-service tools, even well-meaning businesses will fall short. Comment proposes the creation of a publicly accessible online toolkit containing: Compliance checklists for SMEs by industry;	The Agency notes the commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.

		Risk assessment templates; Pre-use notice and privacy policy generators; and FAQs in multiple languages. This approach follows models used by the UK ICO and Colorado Department of Law.	
Costs	463	Comment believes the Agency underestimated implementation and operational costs by excluding out-of-state businesses and ignoring effects of the regulations on ongoing business operations, including negatives to cost and productivity. This underestimates the expense, especially of the regulations around ADMT, whose broad scope and first-in-the-nation impact will dramatically increase California business's ongoing costs.	The Agency disagrees with this comment. The impact of the regulations on foreign businesses and businesses in other states without a physical presence in CA are outside the scope of the SRIA. Government Code § 11346.3(a) requires the SRIA to look at the regulation's impacts on California business enterprises. According to the California Employment Development Department methodology, this means firms with a physical presence in CA. The Agency has made a good faith effort to estimate the costs associated with these regulations on businesses with a physical presence in CA. Also, the Agency recognizes in the SRIA that not every cost can be estimated, which is why the Agency took a more general approach and focused on the areas that it expects to have the highest costs. The Agency made a good faith effort to estimate the costs associated with these regulations given available data.
Costs	481	Comment supports the Agency's conclusion that the November 2024 proposal offers more benefits than harms. Although there are short-term costs, these are outweighed by privacy protections, long-term economic benefits, and reduced harm from cyber incidents.	The Agency agrees with this comment and notes comment's support.
General	64, 173, 342, 343, 429, 515	Comment argues that the timelines for compliance for the amendments to the existing regulations and the risk assessment requirements do not provide sufficient time for the necessary work that must be undertaken to meet these new obligations. Given the scope and breadth of the regulatory package, comment argues that the Agency should afford businesses more than a year to comply with new mandates before they become enforceable. The Agency should clarify that civil and administrative enforcement of new regulatory provisions will not commence until at least one year from the date the provisions are in effect.	The Agency disagrees with this comment. The compliance dates balance the burden on businesses with protections for consumers' privacy. Businesses have additional time to come into compliance with the cybersecurity audit requirements, and with their first risk assessment submissions to the Agency. They also have until January 1, 2027, to comply with Article 11's requirements for certain uses of ADMT. For the other requirements, the Agency does not find convincing the comment's argument for the necessity of additional time. Moreover, straying from the

		Comment expresses concern that the amendments introduce significant new compliance obligations without specifying a timeline. Comment argues that the amendments do not specify compliance deadlines. Comment urges the Agency to provide compliance deadlines. Comment urges the Agency to set January 1, 2027, as the compliance date for all amendments to the existing regulations, to match the ADMT compliance timeline in § 7200(b) and avoid consumer and business confusion. Establishing a compliance date is necessary to provide businesses with a defined deadline to meet the new requirements, which will reduce uncertainty and help businesses allocate their resources accordingly.	APA's established practice for the setting of the effective date would be less effective at protecting consumers' privacy.
General	92	Comment supports the previous exemption in the CCPA/CPRA for employment and employees. Attempting to graft employment concepts into what at its core is a consumer protection law creates confusion and uncertainty for both employees and the regulated employer community. It also potentially doubles enforcement costs and burdens for employers as they attempt to comply with multiple regulatory schemes that all seek to address the same issue.	The Agency disagrees with this comment. The CCPA explicitly provides privacy protections to workers. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, businesses can engage in processing that poses significant risk to privacy in the workplace context, such as through the use of ADMT to make significant employment decisions. The regulations balance providing privacy protections for workers with flexibility for businesses to come into compliance. The regulations are also clear about businesses' obligations and are consistent with other frameworks, which mitigates the risk of confusion or uncertainty.
General	575, 576, 577, 578, 579	Comment critiques DROP regulations. (1) Requiring data brokers to honor deletion requests if more than 50% of the unique identifiers provided match a single consumer record is overly broad and could result in the deletion of personal information for individuals who did not actually submit a request. They also conflict with existing CPPA regulations. For more sensitive information, verification typically requires at least three matching data points before a business is obligated to act. (2) DROP regulations lack sufficient safeguards to verify that authorized agents are legitimately acting on behalf of consumers. This	While not on the proposed action, the Agency notes comment's suggestion and looks forward to continuing to work with stakeholders on future policy development. The Agency encourages commenter to participate in the rulemaking process for the accessible delete mechanism (DROP) regulations.

		omission conflicts with existing CCPA regulations, which require agents to provide signed authorization from the consumer and allow businesses to verify the consumer's identity directly or confirm the authorization. Without similar verification requirements, a significant loophole is created that could be exploited. (3) Regulations do not mandate adequate verification. There is no requirement to confirm that the individual is a California resident and while the regulations allow for verification of specific data elements, they do not require it. This is inconsistent with existing CCPA rules. (4) Require all registered data brokers to reformat their databases to conform to a standardized format could introduce data security risks by enforcing uniform formatting across systems and may also raise First Amendment concerns by compelling how business's structure and maintain their data. (4) Proposed expansion of the "data broker" definition through the revised interpretation of "direct relationship" exceeds the CPPA's regulatory authority. By including entities that have a first-party relationship with consumers—such as those that sell personal information but also directly interact with consumers—the CPPA is contradicting legislative intent. The California Legislature clearly intended to limit data broker registration and compliance obligations to entities that do not have a direct relationship with consumers.	