



February 19, 2025

California Privacy Protection Agency
Attn: Legal Division – Regulations Public Comment
2101 Arena Blvd.
Sacramento, CA 95834

RE: California Consumer Privacy Act Regulations – Nov. 22 Notice of Proposed Rulemaking

Legal Division and Members of the California Privacy Protection Agency,

Thank you for your ongoing consideration of input concerning the Agency’s draft requirements for cybersecurity audits, risk assessments, and access and opt-out rights with respect to automated decisionmaking technology, as well as updates to existing regulations, under the California Privacy Rights Act amendments to the California Consumer Privacy Act (CCPA). The Future of Privacy Forum (FPF) writes to provide perspectives focused on the draft regulations governing automated decisionmaking technology (ADMT) and risk assessments. We offer consideration and recommendations intended to strengthen the proposed regulations by reducing ambiguity and supporting interoperability between California’s regulations with those in other leading U.S. privacy regulatory regimes where practicable.

FPF is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies. FPF seeks to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective regulation.¹

I. Automated Decisionmaking Technology

The California Privacy Protection Agency (CPPA, or the Agency) proposes regulations to establish access and opt-out rights with respect to automated decisionmaking technology. However, these draft regulations include several ambiguities in their scope and definitions which FPF encourages the Agency to clarify before finalizing.

A. The “substantially facilitate” standard for in-scope systems should be amended to provide greater certainty to businesses and ensure that the CCPA takes a risk-focused approach to the use of automated decisionmaking technology.

The Agency should consider providing additional guidance to clarify when use of ADMT amounts to a “key factor” in substantially facilitating human decisionmaking. This could be accomplished either by adding detail to the definition of “automated decisionmaking technology” and/or providing further illustrative examples that distinguish when reliance on ADMT amongst other metrics rises to the level of constituting a “key factor” in a human’s decisionmaking.

As a general matter, one of the most important considerations in assessing the risk posed by an automated decisionmaking system is the degree of influence the system has in contributing to a

¹ The opinions expressed herein do not necessarily reflect the views of FPF’s supporters or Advisory Board.

covered decision or action. There are a broad range of ways that technologies that process personal information can contribute to reaching a decision about an individual. On the low end, a system may simply tabulate data to create an output that amounts to one metric that is part of a broad and varied assessment conducted by a qualified human decisionmaker. At the high end, a system may play a dispositive role, rendering decisions on an automated basis with little to no opportunity for human review or input. Many existing and emerging regulatory frameworks recognize this spectrum by clarifying that the involvement of an automated processing technology that plays a narrow or minor role in the process of making a decision is not high-risk and the decision should not be subject to regulation as an “automated” decision.²

Setting the minimum level of influence that an ADMT system must exercise in rendering covered decisions in order to be in-scope of the law requires careful line drawing and has important practical impacts. If the scope of regulated systems and uses of systems is narrow (e.g., a high threshold that applies only to “solely” automated decisions), then high-risk activities could escape regulation. At the same time, if the scope is too broad (e.g., a low threshold that applies to any use of ADMT that is a “factor” in making a consequential decision), then organizations may be disincentivized from responsibly using beneficial, effective, and efficient technologies or, alternatively be disincentivized from involving qualified human decisionmakers in the decisionmaking process at all, because the use of the system would subject to regulation as an “automated” process either way.

In the context of the draft regulations, the Agency proposes a definition for ADMT that includes “any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or *substantially facilitate* human decisionmaking.”³ In turn, the proposed definition for “substantially facilitate” is “using the output of the technology as a *key factor* in a human’s decisionmaking.”⁴ The regulations further provide an example of in-scope processing involving generating a score that is used as a “*primary factor*” to make a covered decision about an individual.⁵ However, neither the draft regulations nor the Initial Statement of Reasons (ISOR)⁶ provide further guidance for how to evaluate whether the use of an automated system amounts to either a “key factor” or “primary factor” in reaching a covered decision. The Agency should consider providing additional guidance or clarifying examples as to the scope of a key or primary factor, either by elaborating on the definition or providing further examples that distinguish when reliance on ADMT amongst other metrics rises to the level of being a key factor.

² E.g., New York City Local Law 144 Rule, <https://rules.cityofnewyork.us/wp-content/uploads/2023/04/DCWP-NOA-for-Use-of-Automated-Employment-Decisionmaking-Tools-2.pdf> (defining “substantially assist or replace discretionary decision making” narrowly to mean relying on an output with no other factors considered, weighting the output more than other criterion in a set, and using an output to “overrule conclusions derived from other factors including human decision-making”).

³ Cal. Priv. Prot. Agency, Proposed Text of Regulations (October 2024), § 7001(f), https://cppa.ca.gov/meetings/materials/20241004_item3_draft_text.pdf (emphasis added) [*hereinafter* Proposed Text].

⁴ *Id.* (emphasis added).

⁵ *Id.* (emphasis added).

⁶ Cal. Priv. Prot. Agency, Draft Initial Statement of Reasons (October 2024), https://cppa.ca.gov/meetings/materials/20241004_item6_draft_initial_statement_of_reasons [*hereinafter* ISOR].

B. Ensure carveouts for narrowly-used, low-risk AI systems are appropriately tailored to avoid unintended impacts to socially beneficial technologies and use cases.

The draft regulations appropriately recognize and create presumptive (though not absolute) carve outs from the definition of ADMT for certain low-risk, socially beneficial technologies.⁷ In reviewing the technologies on this list, FPF recommends considering additional categorical and technology-specific carve outs.

For the categorical carve out, consider exempting systems that are intended to “[p]erform a narrow procedural task” or “[d]etect decision-making patterns or deviations from prior decision-making patterns” so long as the system “is not intended to replace or influence a previously completed human assessment without sufficient human review.”⁸ The Agency could either exempt such uses or provide that an ADMT does not “substantially facilitate” human decisionmaking when developed and deployed for accomplishing such limited tasks. Adding a categorical carve out such as this will avoid implicating narrow, low-risk applications of AI systems that may not yet be anticipated.

In addition to a categorical carve out, the Agency should also explore additional presumptive exemptions for specific technologies or use cases that are low-risk and socially beneficial. The Agency’s proposed regulations already include a list of some such exemptions. However there are certain technologies that may be worth considering exempting, such as technologies that are exempted from Colorado’s high-risk AI law but are not exempted from the Agency’s proposed regulations, including “anti-fraud technology that does not use facial recognition,” “cybersecurity,” and “technology that communicates with consumers in natural language for the purpose of providing users with information, making referrals or recommendations, and answering questions and is subject to an accepted use policy that prohibits generating content that is discriminatory or harmful.”⁹ The Agency should consider adding these exemptions and other low-risk applications of AI raised by other commenters.

In particular, a specific reference to use of technology for security purposes could give greater clarity to covered organizations. While the regulations recognize important cybersecurity technologies such as firewalls and anti-virus tools, it is ambiguous which other cybersecurity tools or automated tools that can be used for cybersecurity purposes, such as keyword filtering, would qualify as presumptively exempt technologies under the ambiguous “similar technologies” provision.¹⁰

⁷ Proposed Text § 7001(f)(4).

⁸ Colo. Rev. Stat. § 6-1-1701(9)(b) (2025). This exemption comes from Colorado SB 24-205 (2024), a recently enacted law that regulates “high-risk” AI systems that are used to reach, or are significant factors in reaching, consequential decisions. For an overview of Colorado’s law, see Tatiana Rice, Keir Lamont & Jordan Francis, *The Colorado Artificial Intelligence Act: FPF U.S. Legislation Policy Brief* (July 2024), https://fpf.org/wp-content/uploads/2024/07/FPF-Legislation-Policy-Brief_-The-Colorado-AI-Act-Final.pdf.

⁹ Compare Colo. Rev. Stat. § 6-1-1701(9)(b)(II) (2025), with Proposed Text § 7001(f)(4).

¹⁰ Proposed Text § 7001(f)(4).

C. Clarify the intended scope of defining “significant decision” to include decisions that result in “access to” the specified goods and services.

Draft regulations § 7200(a)(1) defines “significant decisions” subject to ADMT notice requirements, access, and opt-out rights:

[A] decision . . . that results in **access to**, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).¹¹

Analogous state comprehensive privacy laws have established protections concerning profiling in furtherance of “decisions that produce legal or similarly significant effects concerning the consumer,” which is often defined as decisions made by the controller “that result in the *provision or denial* by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services.”¹²

The standard definition under the state comprehensive privacy laws closely matches the proposed definition of “significant decision” under these draft regulations. However, the addition of the phrase “access to” is distinct from leading state comprehensive privacy laws’ definitions as well as emerging state AI frameworks, and has unclear impacts: Of the 16 state comprehensive privacy laws that offer a profiling opt-out, all of them use a “provision or denial” standard, with no reference of “access” other than to essential goods or services or basic necessities.¹³ Notably, while the ISOR stresses alignment with federal, state, and international frameworks, laws, and guidance, it does not provide a reason for including the “access to” language or the intended impact.¹⁴

If read literally, this language could bring into scope automated technologies that do not make or influence *decisions*, but instead have a far removed, downstream role in how individuals use technology. For example, including technologies that implicated “access to” important life opportunities could include low-risk and routine systems used to manage ISP network traffic management, or even smart vehicles and trip planning software. There is an alternative, narrower reading of “access to,” however, in which the term would be read as synonymous with provision or denial, though that would render the provision superfluous. Given the plausible alternative readings of the “access to” language, FPF recommends that the Agency remove or clarify the intended scope of this definition.

¹¹ *Id.* § 7200(a)(1) (emphasis added).

¹² Colo. Rev. Stat. Ann. § 6-1-1303 (2025) (emphasis added).

¹³ *Id.*; Conn. Gen. Stat. § 42-515(15) (2024); Del. Code Ann. tit. 6, § 12D-102(13) (2025); Ind. Code § 24-15-2-11 (2024); Ky. Rev. Stat. Ann. § 367.361(10) (2025); S.B. 541, 2024 Reg. Sess., § 14-4601(O) (Md. 2024); Minn. Stat. § 325M.11(i) (2025); Mont. Code Ann. § 30-14-2802(10) (2025); Neb. Rev. Stat. § 87-1102(11) (2025); N.H. Rev. Stat. Ann. § 507-H:1(XIII) (2025); N.J. Stat. Ann. § 56:8-166.4 (2025); Or. Rev. Stat. § 646A.570(10) (2025); R.I. Gen. Laws § 6-48.1-2(12) (2025); Tenn. Code Ann. § 47-18-3302(10) (2025); Tex. Bus. & Com. Code Ann. § 541.001(11) (2025); Va. Code Ann. § 59.1-575 (2025).

¹⁴ See ISOR, p. 80-81.

D. Application of requirements to training ADMT systems that are “capable” of being used for designated purposes under §§ 7150(b)(4) & 7200(a)(3) may be an overly broad standard.

Under the proposed regulation, businesses will be required to conduct a risk assessment for certain “training uses” of ADMT or AI. “Training uses” means:

Processing the personal information of consumers to train automated decisionmaking technology or artificial intelligence that is **capable** of being used for any of the following:

- (A) For a significant decision concerning a consumer;
- (B) To establish individual identity;
- (C) For physical or biological identification or profiling;
- (D) For the generation of a deepfake; or
- (E) For the operation of generative models, such as large language models.¹⁵

Businesses will also be required to offer opt-out rights for the above training uses, except for (E).¹⁶

Application of these obligations and rights to the use of personal information to train ADMT and AI systems that are “capable of” being used for the listed purposes would create ambiguity regarding which ADMT or AI systems are within scope. This is because many systems could plausibly be used for various purposes for which they are neither intended nor fit to be used. For example, any basic AI technology, such as chatbots or spreadsheets, could arguably be “capable” of rendering significant decisions impacting consumers depending on downstream use.¹⁷ Requiring businesses to assess risks on every possible use and misuse of a system by unknown third party recipients of the technology prior to development will lead to excessive assessments disconnected from actual risks to individuals, even for the development of systems that are not intended to or likely to be used for any of the listed training purposes.

The Agency could change the standard to apply to processing personal information to train ADMT or AI systems that are “intended” to be used for the listed purposes. An alternative option, if limitation to “intended” uses is stricter than the Agency prefers, would be to limit the regulations’ application to “reasonably likely” or “reasonably foreseeable” uses of the ADMT or AI system. Such an assessment would still be subjective from the business’s perspective in the same way that identifying “capable” uses is subjective, but this heightened standard would insulate businesses from projecting every possible use and misuse of a given system and instead return focus to anticipating likely applications.

E. In §§ 7150(b)(4)(B) & 7200(a)(3)(B), clarify what it means for an ADMT or AI system to be used for “establish[ing] individual identity.”

The covered “training uses” of ADMT and AI subject to risk assessment obligations and ADMT access and opt-out rights include processing personal information to train ADMT or AI systems

¹⁵ Proposed Text § 7150(b)(4) (emphasis added).

¹⁶ *Id.* § 7200(a)(3).

¹⁷ For an analog analogy, a Magic 8 Ball is “capable” of being used to make decisions implicating an individual’s employment such as hiring, termination, and promotion, but are not be regulated as employment decisionmaking tools.

that are capable of being used to both (1) “establish individual identity” and (2) for “physical or biological identification.”¹⁸ While the proposed regulations define “physical or biological identification or profiling,” the regulations do not define, and the ISOR offers no guidance on how “establishing individual identity” is a distinct use case of ADMT.¹⁹ The Agency should consider either removing or providing a definition of this term and clarifying how it is distinct from “physical or biological identification.”

F. Clarify that requests to opt-out of ADMT after the business has initiated processing do not require retraining of models under § 7221(n).

Under §7221(n), if a person submits a request to opt-out of ADMT after the business has initiated the processing, the business is required to cease processing that person’s personal information using that ADMT, neither use nor retain personal information previously processed by that ADMT, and pass on the opt-out to service providers, contractors, and other persons to whom the business disclosed or made personal information available to process using that ADMT.²⁰

FPF notes that there may be differing practical realities and policy considerations across the range of ADMT technologies and use cases to which opt-out rights apply (significant decisions, work or educational profiling, training of ADMT). An opt-out right that requires ceasing use of ADMT to process an individual’s information on a forward looking basis to reach significant decisions or for extensive profiling is consistent with the CCPA’s general approach to opt-out rights. However, there may be additional practical complications to applying a backward looking right to opt out of processing for training uses of ADMT where training has already begun or occurred. This is especially pertinent given ongoing technical and legal uncertainty under what conditions personal information can be said to be found in model weights or otherwise is continued to be processed by some AI models after training occurs.²¹ The Agency should clarify whether there are circumstances under which this provision would require the developer of an AI system to retrain a model that was trained on a person’s personal information before that person submitted an opt-out request or whether this provision merely prevents future training utilizing the personal information in question.

II. Risk Assessments

As of February 2025, seventeen U.S. states have enacted comprehensive privacy laws which currently—or will upon taking effect—require covered entities to conduct and document assessments of the risk of certain data processing activities. As FPF noted in pre-rulemaking comments to the Agency, “[d]ata protection assessments are an important tool for ensuring that organizations consider privacy implications and safeguards in the development of products and

¹⁸ *Id.* §§ 7150(b)(4)(B) & 7200(a)(3)(B).

¹⁹ *Id.* § 7001(gg) (“‘Physical or biological identification or profiling’ means identifying or profiling a consumer using information that depicts or describes their physical or biological characteristics, or measurements of or relating to their body. This includes using biometric information, vocal intonation, facial expression, and gesture (e.g., to identify or infer emotion).”).

²⁰ *Id.* § 7221(n).

²¹ See Jordan Francis, Beth Do & Stacey Grey, *Do LLMs Contain Personal Information? California AB 1008 Highlights Evolving, Complex Techno-Legal Debate*, FPF (Oct. 25, 2024), <https://fpf.org/blog/do-llms-contain-personal-information-california-ab-1008-highlights-evolving-complex-techno-legal-debate> (discussing the topic of personal information in AI systems in the contexts of LLMs).

services while also providing for a record that allows organizations to demonstrate compliance efforts.”²²

FPF writes to identify two potential ambiguities in the proposed risk assessment requirements. First, the requirement to identify “technology to be used in the processing” is ambiguous and likely overly broad. Second, the prohibition on commencing processing activities if the risks to consumers’ privacy are outweighed by the benefits of the activity should explicitly provide for consideration of the safeguards that the business has or will implement to mitigate privacy risks.

Furthermore, attached as an appendix to these comments is a chart that compares the risk assessment portion of these proposed regulations against the finalized data protection assessment requirements under the Colorado Privacy Act regulations and the data protection impact assessment requirements under the European Union’s General Data Protection Regulation (GDPR). As the Agency considers interoperability between different privacy frameworks and accepting risk assessments originally completed pursuant to another law, this chart provides an overview of similarities and divergences between the draft regulations and existing regimes.

A. The requirement to identify “technology to be used in the processing” under § 7152(a)(3)(g) is overly broad.

Under draft section 7152, when conducting and documenting a risk assessment, a business must identify certain “operational elements of its processing,” including “[t]he technology to be used in the processing.”²³ In certain contexts, there can be public policy benefits to organizations identifying and disclosing the components of a product or service.²⁴ However, requiring businesses to identify any technology to be used in processing is overinclusive and divorced from an assessment of the actual risks. For example, this provision would, on its face, potentially encompass and require businesses to provide the Agency with a list of everything from individual components of personal computers and network infrastructure, on the one hand, to pencils and other writing implements, on the other hand.²⁵ Furthermore, the technology used in processing is subject to constant change as businesses acquire new hardware and software.

A contrasting approach is that taken under the Colorado Privacy Act regulations. Under Rule 8.04(A)(4), controllers must include in a data protection assessment:

²² Keir Lamont, Future of Privacy Forum Comments, PR 02-2023, (Mar. 27, 2023), https://cppa.ca.gov/regulations/pdf/rm2_pre_comments_27_52.pdf#page=137 (citing Information Commissioner’s Office, *Guide to Data Protection Impact Assessments*, “What is a DPIA?”, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/#dpia2>).

²³ Proposed Text § 7152(a)(3)(G).

²⁴ See e.g., Nat’l Inst. of Sci. & Tech., *Software Security in Supply Chains: Software Bill of Materials (SBOM)*, <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1>.

²⁵ This analysis of the overinclusivity of the term “technology” does not extend to the requirements of § 7152(a)(3)(g)(i)-(ii) that businesses identify the logic and output of automated decisionmaking technology used for purposes identified in § 7150(b)(3).

The nature and operational elements of the Processing activity. In determining the level of detail and specificity to provide pursuant to this section, the Controller shall consider the type, amount, and sensitivity of Personal Data Processed, the impacts that operational elements will have on the level of risk presented by the Processing activity, and any relevant unique relationships. Relevant operational elements may include: . . . b. Technology or Processors to be used.²⁶

Colorado's approach is more flexible and tied to context as the requirements are scaled to the nature of the processing activity. The Agency could soften its requirement by making identification of technology involved in the processing conditional on the technology in question having a bearing on the level of risk presented by the processing activity. Such a requirement would push businesses to disclose use of especially risky and novel technologies while not requiring detailed inventories of every component of the business's tech stack.

B. The prohibition in § 7154 against processing if the risks to consumers' privacy outweigh the processing activity's benefits should explicitly provide that the test requires balancing the risks to consumers' privacy, *as mitigated by safeguards*, against the activity's benefits.

In conducting a risk assessment, businesses must identify both “the negative impacts to consumers' privacy associated with the processing” and “the safeguards that it plans to implement to address the negative impacts identified.”²⁷ However, under § 7154, a business is prohibited from processing personal information for any activity subject to a risk assessment “if the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public from the processing.”²⁸ According to the ISOR, one of the justifications for including § 7154 is that “[i]t benefits businesses by providing a clear articulation of the goal of their risk assessments, and benefits consumers by ensuring that their personal information is not processed in ways that pose unnecessary *and unmitigated* risks to their privacy.”²⁹ However, as currently drafted, this provision is ambiguous as to whether that calculus accounts for mitigations and safeguards implemented or planned to be implemented by the business to reduce risks to consumers' privacy.

Colorado's data protection assessment regulations, in contrast, explicitly account for safeguards in their balancing test:

At a minimum, a data protection assessment must include the following information: . . . A description of how the benefits of the Processing outweigh the risks identified pursuant to 4 CCR 904-3, Rule 8.04(A)(6), *as mitigated by the safeguards identified* pursuant to 4 CCR 904-3, Rule 8.04(A)(7).³⁰

²⁶ 4. Colo. Code Reg. 904-3, Rule 8.04(A)(4) (2023).

²⁷ Proposed Text § 7152(a)(5)-(6).

²⁸ *Id.* § 7154.

²⁹ ISOR, at p.73 (emphasis added).

³⁰ 4. Colo. Code Reg. 904-3, Rule 8.04(A)(8) (2023) (emphasis added). Although this language appears to presume that benefits outweigh the risks, the regulation further requires that data protection assessments be “genuine,” “thoughtful,” and *demonstrate* that “the benefits of the Processing outweigh the risks offset by safeguards in place.” *Id.* Rule 8.01.

Although this may be an implicit assumption of the balancing test written in § 7154—that risks to consumers’ privacy mean those risks that remain after mitigations—the Agency could adopt language similar to Colorado’s and rewrite § 7154 to unambiguously account for safeguards.

III. Cybersecurity Audits

A. Consider whether a board member is the most appropriate party to certify a business’s cybersecurity audits.

The draft regulations would require that cybersecurity audits be reported to a business’s board of directors and include a statement signed and dated by a member of the board.³¹ Within this statement, the board member must certify that they have reviewed and understand the findings of the cybersecurity audit. While a board member may be equipped to certify to *receiving* an audit, or capable of determining if all of the elements of an audit are present, a board member is unlikely to be best positioned within an organization to certify that they understand the *findings* of a cybersecurity audit.

As explained in the ISOR, if a business does not have a board or governing body, the business’s highest-ranking executive with authority to certify on behalf of the business and who is responsible for its cybersecurity program may complete this statement.³² If the Agency chooses to maintain the requirement that audits must be certified by a member of the business, the Agency could consider certification by a person with relevant authority in cybersecurity for all businesses, rather than only ones that do not have a governing board.³³

IV. Updates to Existing Regulations

A. Provide flexibility to support the delivery of effective and context-appropriate privacy notices.

The draft regulations provide that privacy notices required for immersive reality tools, such as augmented or virtual reality, must be provided in a “manner that ensures that the consumer will encounter the notice before the consumer enters the augmented or virtual reality environment.”³⁴ The ISOR provides that the intent of this section is to ensure that “the notice is effective in informing consumers of their right[s].”³⁵ However, the draft regulations introduce confusion about where and how such notices must be provided, in part because the regulated “environment” appears to encompass immersive technologies at both the platform (“gaming devices”) and application (“mobile applications”) level.

Virtual and augmented reality devices, by design, immediately bring users into an immersive environment even before they enter a specific application. As such, it is unclear how a user would

³¹ Proposed Text § 7122(h)-(i).

³² ISOR p. 48 https://cppa.ca.gov/meetings/materials/20241004_item6_draft_initial_statement_of_reasons

³³ Amie Stepanovich, *Challenges and Opportunities in Organizational Collaboration on Privacy and Cybersecurity* (Nov. 2024), https://fpf.org/wp-content/uploads/2024/11/Challenges-and-Opportunities-in-Organizational-Collaboration-on-Privacy-and-Cybersecurity_FINAL.pdf.

³⁴ Proposed Text §§ 7013(e)(3)(D) & 7014(e)(3)(D).

³⁵ ISOR p. 28.

be shown a notice *before* entering the regulated environment, unless notice was provided on a separate device. A consumer may also have already entered an augmented or virtual environment platform when encountering a business for the first time (for example, using an app store in a virtual environment). Given the plausible device-level interpretation of “environment,” the draft regulations could require that an individual must exit their virtual or augmented reality environment platform, engage with notices, and then re-enter the virtual or augmented reality platform before proceeding with their desired use or interaction with a business’s application. It is unclear whether disrupting a user experience in this manner would make a notice more effective.

Furthermore, the ISOR does not explain why a notice offered in an augmented or virtual reality environment is considered to be *per se* less effective than a notice conveyed outside an augmented or virtual reality environment. In fact, there is potential that, properly designed, notices in AV/VR contexts may be just as, if not more, effective than traditional disclosures, given that these environments offer new and substantial dynamic opportunities to present an individual with information. FPF recommends that the regulations should ensure flexibility in order to provide context appropriate and timely notices, as regulations should focus on quality of notices, not necessarily the format in which notices are provided.

* * *


Thank you for this opportunity to provide comment on these proposed regulations. We welcome any further opportunities to provide resources or information to assist in this important effort.


Sincerely,


Jordan Francis
Policy Counsel, U.S. Legislation & Regulation
jfrancis@fpf.org


Keir Lamont
Senior Director, U.S. Legislation & Regulation
klamont@fpf.org


<div>  <div>Comparison of Risk Assessment Requirements: California, Colorado & European Union</div> </div>				
	CCPA Draft Regulations	Colorado Privacy Act Regulations	General Data Protection Regulation	FPF Analysis - California v. Colorado
References	<p>Proposed Risk Assessment Regulations (to be codified at Cal. Code Reg. tit. 11, art. 10)</p> <p>Cal. Civ. Code § 1798.185, subd. (a)(15)</p>	<p>4 Colo. Code Regs. § 904-3, Parts 8 & 9</p> <p>Colo. Rev. Stat. § 6-1-1309</p>	<p>General Data Protection Regulation (GDPR), Article 35</p> <p>EDPB Guidelines on DPIAs</p>	<p>This comparison chart focuses on the California Privacy Protection Agency's proposed regulations (Nov. 2024) and comparable benchmarks under the Colorado Privacy Act regulations. Of the various US states with data protection assessment requirements currently in effect, Colorado was selected for this chart as having the most prescriptive requirements. Note 1: In 2024, Colorado enacted Senate Bill 41, which added new data protection assessment requirements for controllers that offer any online service, product, or feature to a consumer whom such controller actually knows or willfully disregards is a minor if that online product, service, or feature creates a heightened risk of harm to minors. Those data protection assessment requirements are outside the scope of this comparison chart. Note 2: The GDPR's relevant DPIA requirements are provided for additional comparison, but GDPR is not addressed in the analysis column, to keep the analysis focused on U.S. state privacy law.</p>
What is the assessment called?	Risk assessment (RA)	Data protection assessment (DPA)	Data protection impact assessment (DPIA)	The majority of enacted state comprehensive privacy laws use the term data protection assessment.
When, generally, is an assessment required?	<p>Processing consumers' personal information (PI) that presents significant risk to consumers' privacy.</p> <p>Cal. Civ. Code § 1798.185, subd. (a)(15); Draft § 7150.</p>	<p>Processing of personal data (PD) that presents a heightened risk of harm to a consumer.</p> <p>C.R.S. § 6-1-1309(1).</p>	<p>Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.</p> <p>Art. 35(1).</p>	<p>DPIAs are required where processing activities pose some heightened risk of harm.</p> <p>Exhaustive or Open: An important difference is whether these lists are exhaustive. California's list is exhaustive. RAs are only required if a processing activity is listed in § 7150(b), but the Agency can add more activities in the future. Colorado, in contrast, has an open standard with an illustrative list of processing activities that meet the threshold.</p>
Are there specific processing operations that meet the risk/harm threshold?	<p>Yes, the following processing activities present significant risk to consumers' privacy:</p> <p>(1) Selling or sharing PI; (2) Processing sensitive PI (employment exceptions); (3) Using automated decisionmaking technology (ADMT) for a significant decision[*] concerning a consumer or for extensive profiling^{**} (4) Processing consumers' PI to train ADMT or artificial intelligence (AI) capable of being used for: (A) a significant decision concerning a consumer, (B) establishing individual identity, (C) physical or biological identification or profiling, (D) deepfake generation, or (E) the operation of generative models (e.g., LLMs).</p> <p>Draft § 7150(b).</p> <p>[*] A decision that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).</p> <p>^{**} Includes profiling through (i) systematic observation when they are acting in certain capacities (student, employee, etc.), (ii) systematic monitoring of a publicly accessible place, or (iii) profiling for behavioral advertising.</p>	<p>Yes, processing that presents a heightened risk of harm to a consumer includes:</p> <p>(a) Processing PD for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of: (I) unfair/deceptive treatment of, or unlawful disparate impact on, consumers, (II) financial or physical injury to consumers, (III) intrusion upon solitude / seclusion / private affairs or concerns of consumers if such would be offensive to a reasonable person, or (IV) other substantial injury to consumers; (b) Selling PD; (c) Processing sensitive data.</p> <p>C.R.S. § 6-1-1309(2).</p> <p>Rule 9.06 defines "unfair or deceptive treatment" and "unlawful disparate impact."</p>	<p>Yes, high risk processing activities include:</p> <p>(a) Automated processing, including profiling,[†] leading to decisions that produce legal effects concerning the subject or similarly significantly affect them; (b) Large scale processing of special category data (Art. 9(1)) or personal data (PD) relating to criminal convictions and offences (Art. 10)); or (c) Large scale systematic monitoring of publicly accessible areas.</p> <p>Supervisory authorities must establish public lists of processing operations that require a DPIA and can establish lists of processing operations that do not require a DPIA.</p> <p>EDPB Guidelines recommend conducting a DPIA where at least two of the nine following criteria are met:</p> <ul style="list-style-type: none"> • Evaluation or scoring; • Automated decisionmaking with legal or similar significant effect; • Systematic monitoring; • Sensitive data or data of a highly personal nature; • Data processed on a large scale^{††}; • Matching or combining datasets; • Data concerning vulnerable data subjects; • Innovative use or applying new technological or organizational solutions; and • When processing prevents data subjects from exercising a right or using a service or a contract. <p>Art. 35(3) & (4); EDPB Guidelines on DPIAs, at pages 9–11. [†] See Recital 71; ^{††} See Recital 91.</p>	<p>Profiling and ADMT: California and Colorado take different approaches with respect to profiling and ADMT. California requires RAs for ADMT used to make significant decisions, for extensive profiling, or for processing PI to train ADMT/AI capable of being used for certain purposes. This is more specific and granular than Colorado's approach, which requires DPIAs for profiling that presents a reasonably foreseeable risk of certain injuries (e.g., unfair or deceptive treatment, financial injury). Drilling down into the harms to consider in a DPA, these approaches might be closer than they appear. For example, California requires businesses to consider risks like discrimination and economic harms, similar to Colorado's profiling trigger, and Colorado requires controllers to consider harms such as denial of a right or privilege such as housing or employment, which is similar to California's significant decisions trigger.</p> <p>Public Monitoring: California is unique amongst U.S. state privacy laws in requiring RAs for certain types of public monitoring and first party behavioral advertising.</p> <p>Adolescent Privacy: California and Colorado both require assessments for processing sensitive data. In California, the proposed updated draft regulations would expand the definition of sensitive personal information to cover personal information of consumers whom the business has actual knowledge are under 16. This is broader than Colorado's approach, which defines as sensitive the personal data from a known child (under 13).</p>

<div>  <div>Comparison of Risk Assessment Requirements: California, Colorado & European Union</div> </div>				
	CCPA Draft Regulations	Colorado Privacy Act Regulations	General Data Protection Regulation	FPF Analysis - California v. Colorado
Which stakeholders should be involved?	<p>Required: All <i>relevant</i> individuals. Role in the assessment is based on involvement in the processing activity subject to assessment.</p> <p>Optional: External parties (such as service providers, contractors, ADMT bias experts, subset of affected individuals, stakeholders representing individuals' or others' interests (e. g., consumer advocacy groups). Consulting external parties to ensure current knowledge of emergent privacy risks and countermeasures is a safeguard that a business may consider in an assessment.</p> <p>Draft §§ 7151, 7152(a)(6)(A)(iii).</p>	<p>DPA's must involve <i>all relevant internal actors</i> and, "where appropriate," <i>relevant external parties</i>.</p> <p>Rule 8.03(A).</p>	<p>The controller shall seek the advice of the data protection officer, where designated, when carrying out a DPIA, and, where appropriate, shall seek the views of data subjects.</p> <p>A controller shall consult a supervisory authority where a DPIA indicates that processing involves a high risk which cannot be mitigated by appropriate measures, or whenever member state law requires consultation before a controller carries out processing for the performance of a task in the public interest.</p> <p>Art. 35(2) & (9); Art. 36(1) & (5); Recital 84.</p>	<p>Both regimes require input from relevant internal actors. California encourages consulting with affected individuals where appropriate; Colorado does not address this.</p> <p>This row omits information on whether service providers / processors are required to assist businesses / controllers in conducting assessments.</p>
Do assessment requirements scale?	Not explicitly.	<p>Yes. The depth, level of detail, and scope of DPA's should take into account the scope of risk presented, size of the controller, amount and sensitivity of PD processed, PD processing activities subject to the assessment, and complexity of safeguards applied.</p> <p>Rule 8.02(C).</p>	<p>Not explicitly. The text of the GDPR does not make any differentiation based on the size of the controller, while Guidelines from the EDPB highlight that the implementation of a DPIA is scalable to the processing operations of even a "small data controller". The complexity of the processing operations and level of risk to the rights of individuals are the key factor to impact the complexity of a DPIA.</p> <p>EDPB Guidelines on DPIAs, at page 17.</p>	Colorado includes an explicit statement that assessments should be tailored to the complexity and risk of the processing operations under consideration or the size of the business.
Are there exceptions?	<ul style="list-style-type: none"> Processing consumers' sensitive PI does not require a RA if the business is processing the sensitive PI of its employees or independent contractors "solely and specifically for purposes of administering compensation payments, determining and storing employment authorization, administering employment benefits, or wage reporting as required by law, is not required to conduct a risk assessment for the processing of sensitive personal information for these purposes." Using ADMT for a significant decision concerning a consumer or for extensive profiling does not include decisions made using information subject to the exceptions set forth in Cal. Civil Code §§ 1798.145, subd. (c)-(g), or 1798.146, subd. (a)(1), (4), and (5). 	No.	<p>Yes, when the lawful basis for processing is Art. 6(1)(c) [compliance with a legal obligation] or (e) [performance of a task carried out in the public interest or in the exercise of official authority vested in the controller], and that obligation is based in E.U. law or the law of a Member State, and a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, then Art. 35(1)–(7) shall not apply unless a Member State deems it necessary to do so prior to processing. Additionally, Member States have the ability to whitelist certain processing operations.</p> <p>Art. 35(10); Art. 35(5).</p>	For California and Colorado, data-level and entity-level exceptions to the underlying laws will apply to the regulations as well. The CCPA is broader than the Colorado Privacy Act in that it applies to employee and business-to-business data.
What are the substantive elements of an assessment? [See below for elements specific to AI, ADMT, & Profiling]	<p>(1) <i>Specifically identify the purpose for processing PI</i>;</p> <p>(2) Identify categories of PI to be processed (including whether they include sensitive PI);</p> <p>(3) Identify certain operational elements* of the processing;</p> <p>(4) <i>Specifically identify benefits to the business, consumer, other stakeholders, and public</i> from the processing;</p> <p>(5) <i>Specifically identify negative impacts* to consumers' privacy</i>;</p> <p>(6) Identify safeguards* the business plans to implement to address the identified negative impacts;</p> <p>(7) Identify whether the business will initiate the processing subject to the RA;</p> <p>(8) Identify the contributors to the RA;</p> <p>(9) Identify the date the RA was reviewed and approved; and names and positions of individuals responsible.</p> <p>Draft § 7152.</p> <p>* Specified in draft regulation</p>	<p>DPA's must identify and describe the risks to consumers' rights associated with the processing, document measures considered and taken to address and offset risks, contemplate the processing's benefits, and demonstrate that benefits outweigh the risks as offset by safeguards. Specific elements:</p> <p>(1) Short summary of the processing activity;</p> <p>(2) Categories of PD to be processed (including whether they include sensitive data and data from a known child);</p> <p>(3) Context of the processing activities (including the controller's and consumers' relationship and consumers' reasonable expectations);</p> <p>(4) Nature and operational elements of the processing;</p> <p>(5) Core purposes of the processing activity and other benefits that may flow, directly or indirectly, to the controller, consumer, other stakeholders, and the public;</p> <p>(6) Sources and nature of risks to the rights of consumers;</p> <p>(7) Safeguards to be employed to reduce identified risks;</p> <p>(8) Description of how the benefits outweigh the risks (as mitigated by safeguards);</p> <p>(9) For profiling (see C.R.S. § 6-1-1309(2)(a)), the DPA must also comply with Rule 9.06 (see below);</p>	<p>In conducting a DPIA, a controller should take into account the nature, scope, context and purposes of the processing and the sources of risk.</p> <p>DPIAs shall contain at least:</p> <p>(a) A description of the envisaged processing operations and the purposes of the processing;</p> <p>(b) An assessment of the necessity and proportionality of the processing;</p> <p>(c) An assessment of the risks to the rights and freedoms of data subjects; and</p> <p>(d) Measures envisaged to address the risks and demonstrate GDPR compliance.</p> <p>Art. 35(7); Recital 90.</p> <p>Note: The assessment of the risks to the rights and freedoms of data subjects is broader than just "privacy" risks. Rather, it concerns all rights and freedoms that may be impacted by the processing operations, which may include freedom of speech, due process, non-discrimination, etc.</p> <p>EDPB Guidelines on DPIAs, at page 6.</p>	<p>Operational Elements: One notable difference between California and Colorado is the level of specificity required in detailing operational elements of the processing. The Colorado regulations afford controllers some flexibility in determining the level of detail and specificity to provide, and list relevant operational elements that may be included.</p> <p>Weighing Risks and Benefits: Another notable difference is the framing of the ultimate balancing test. Both California and Colorado prohibit a processing activity if the risks outweigh the benefits. Section 7154 of the proposed regulations, however, provide that a business "must not process personal information for any processing activity identified in section 7150, subsection (b), if the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public from the processing." Colorado, in contrast, provides more flexibility to controllers, instead requiring that they include a "description" of how the benefits outweigh the risks as mitigated by safeguards. Given the inherent difficulty in quantifying and comparing risks and benefits in this context, Colorado's standard could ease concerns about good faith estimates of the balance of risks and benefits being second guessed.</p>

<div>  <div> <div>Comparison of Risk Assessment Requirements: California, Colorado & European Union</div> </div> </div>				
	CCPA Draft Regulations	Colorado Privacy Act Regulations	General Data Protection Regulation	FPF Analysis - California v. Colorado
		<p>(10) For processing sensitive data, details of the process implemented to ensure that PD and sensitive data inferences are not transferred and are deleted with 24 hours of the processing activity;</p> <p>(11) Relevant internal actors and external parties contributing to the DPA;</p> <p>(12) Any internal/external audit conducted for the DPA, including details about the auditor or individuals involved;</p> <p>(13) Dates DPA was reviewed and approved; and names, positions, and signatures of those responsible.</p> <p>Rule 8.02(A); Rule 8.04.</p>		
What harms/risks should be considered?	<p>Negative impacts to consumers' privacy include:</p> <p>(A) Security harms (e.g., unauthorized access);</p> <p>(B) Discrimination on the basis of protected classes;</p> <p>(C) Impairing consumers' control over their PI;</p> <p>(D) Coercing or compelling consumers into allowing processing of their PI;</p> <p>(E) Disclosing a consumer's media consumption in a manner that chills or deters speech, expression, or exploration of ideas;</p> <p>(F) Economic harms;</p> <p>(G) Physical harms to consumers or property;</p> <p>(H) Reputational harms;</p> <p>(I) Psychological harms;</p> <p>Draft § 7152(a)(5).</p>	<p>Risks to the rights of consumers may include:</p> <p>(a) Constitutional harms;</p> <p>(b) Intellectual privacy harms;</p> <p>(c) Data security harms;</p> <p>(d) Discrimination harms;</p> <p>(e) Unfair, unconscionable, or deceptive treatment;</p> <p>(f) A negative outcome/decision with respect to an individual's eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services;</p> <p>(g) Financial injury or economic harm;</p> <p>(h) Physical injury, harassment, or threat to an individual or property;</p> <p>(i) Privacy harms, such as intrusion upon solitude/seclusion/private affairs or concerns of consumers, stigmatization, or reputational injury;</p> <p>(j) Psychological harm;</p> <p>(k) Other detrimental or negative consequences that affect an individual's private life or similar concerns where an individual has a reasonable expectation that personal data or other data will not be collected, observed, or used.</p> <p>Rule 8.04(A)(6).</p>	<p>Risk to the rights and freedoms of natural persons may result from personal data processing which could lead to physical, material or non-material damage, resulting from the following processing operations / situations:</p> <ul style="list-style-type: none"> • Processing that may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of PD protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; • Where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their PD; • Where PD are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; • Where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; • Where PD of vulnerable natural persons, in particular of children, are processed; or • Where processing involves a large amount of PD and affects a large number of data subjects. <p>Recital 75.</p>	<p>California and Colorado have a slight difference in approach tied to the triggers for an assessment (see above). For example, Colorado requires DPAs for uses of profiling that present a reasonably foreseeable risk of certain injuries and then considers a negative outcome with respect to an individual's eligibility for a right, privilege, or benefit to be a harm worth considering. California instead treats the use of ADMT to make a significant decision as a trigger for a DPA, then requires consideration of harms such as economic injury or discrimination.</p>
What safeguards should be considered?	<p>Safeguards a business may consider include:</p> <p>(i) Encryption, segmentation, access controls, change management, network monitoring and defenses, and data and integrity monitoring;</p> <p>(ii) Use of PETs (e.g., trusted execution environments, federated learning, homomorphic encryption, differential privacy);</p> <p>(iii) Consulting external parties to ensure current knowledge of emergent privacy risks and countermeasures;</p> <p>(iv) Evaluating need for human involvement in use of ADMT and implementing such as necessary;</p> <p>Draft § 7152(a)(6)(A).</p>	<p>Measures considered shall include:</p> <p>(a) Use of de-identified data;</p> <p>(b) Measures taken pursuant to controller duties (e.g., data minimization, avoiding secondary use, etc.), including an overview of data security practices implemented, data security assessments completed, and measures taken to comply with consent requirements.</p> <p>(c) Measures taken to ensure consumers have access to rights provided in C.R.S. § 6-1-1306 (opt-out, access, correction, deletion, data portability).</p> <p>Rule 8.04(A)(7).</p>	<p>EDPB Guidelines provide examples of measures that can be appropriate safeguards, such as:</p> <ul style="list-style-type: none"> • Pseudonymization; • Encryption of PD; • Data minimization; • Oversight mechanisms; etc. <p>EDPB Guidelines on DPIAs, at 19.</p>	<p>California and Colorado both provide examples of safeguards to consider but neither require that those specific safeguards be implemented.</p>
Do assessments prohibit certain processing activities?	<p>Yes. If the risks to consumer's privacy outweigh the benefits resulting from processing (to the consumer, business, other stakeholders, and public), then the business shall not process PI for that activity.</p> <p>Draft § 7154.</p>	<p>Yes. A DPA must "demonstrate[] that the benefits of the Processing outweigh the risks offset by safeguards in place."</p> <p>Rule 8.02(A).</p>	<p>Unclear. There is no explicit statement not to engage in processing if the risks outweigh the benefits, but there is a requirement to consult with a supervisory authority if risks cannot be mitigated. The supervisory authority may use its Art. 58 powers if it determines that the intended processing would infringe the GDPR.</p> <p>Art. 36; Recital 84.</p>	<p>California and Colorado both explicitly say that for processing to proceed the benefits must outweigh the risks as offset or mitigated by applicable safeguards.</p>
What is the timing for conducting an assessment?	<p>Before initiating any processing activity that presents a significant risk to consumers' privacy.</p> <p>Draft § 7155(a)(1).</p>	<p>Before initiating a processing activity that presents a heightened risk of harm to a consumer.</p> <p>Rule 8.05(A).</p>	<p>Before initiating processing that is likely to result in a high risk to the rights and freedoms of natural persons.</p> <p>GDPR Recital 90.</p>	<p>This differs from the majority of enacted US state comprehensive laws who, with the exception of New Jersey, do not explicitly require that the assessment occur <i>before</i> initiating processing. Such a requirement could raise First Amendment challenges.</p>

 Comparison of Risk Assessment Requirements: California, Colorado & European Union				
	CCPA Draft Regulations	Colorado Privacy Act Regulations	General Data Protection Regulation	PPF Analysis - California v. Colorado
When should assessments be updated?	<p>Material changes: Update a RA immediately whenever there is a material change¹ in the processing activity.</p> <p>In general: Review, and update as necessary, at least once every three years.</p> <p>Draft § 7155(a)(2)–(3).</p> <p>¹ A change is material if it diminishes the benefits, creates new negative impacts, increases the magnitude / likelihood of negative impacts, or diminishes the effectiveness of safeguards.</p>	<p>Material changes: A DPA shall be updated when existing processing activities are modified in a way that materially changes the level of risk presented (example list provided in Rule).</p> <p>In general: Review and update DPA as often as appropriate throughout the processing activity's lifecycle, to: (1) monitor for harm caused by the processing and adjust safeguards; and (2) ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing.</p> <p>Profiling: DPAs for profiling in furtherance of decisions that produce legal of similarly significant effects concerning a consumer shall be reviewed and updated at least annually, with an updated evaluation for fairness and disparate impact.</p> <p>Rule 8.05(C) & (D).</p>	<p>Change of risk: A controller shall carry out a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk presented by processing operations.</p> <p>EDPB Guidelines suggests that DPIAs should be continuously reviewed and regularly reassessed.</p> <p>Art. 35(11); EDPB Guidelines on DPIAs, at page 14.</p>	<p>Material Changes: Both regimes require that assessments be updated when there is a sufficient change in the risk posed, which can happen due to technological, society, or organizational reasons.</p> <p>Cadence: These regimes differ as to whether assessments should be regularly reviewed and updated. California is considering a set cadence of once every 3 years to review and update DPAs. Colorado opted for the flexible standard that assessments be updated as appropriate.</p> <p>ADMT / Profiling: Another difference between regimes is whether DPAs regarding ADMT or profiling are singled out for special update requirements. California does not have ADMT- or profiling- specific update requirements, whereas Colorado requires annual review and updates for assessments concerning profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.</p>
How long do you retain assessments?	<p>Retain RAs (originals and updated versions) for as long as the processing continues or five years after the completion of the RA, whichever is later.</p> <p>Draft § 7155(b).</p>	<p>Retain DPAs (including prior versions which have been revised when a new processing activity is generated) for as long as the processing continues and at least three years after the activity's conclusion. Retain DPAs in an electronic, transferable form.</p> <p>Rule 8.05(E).</p>	<p>There is no explicit requirement to retain DPIAs for a certain amount of time after a processing activity concludes, but a controller is still subject to general record-keeping obligations to demonstrate GDPR compliance.</p> <p>See Art. 24.</p>	<p>California is slightly stricter than Colorado, requiring that assessments be retained for two years longer.</p>
Are retroactive assessments required?	<p>Yes. A business has 24 months to conduct a RA for covered processing activities initiated prior to the effective date that continue after the effective date.</p> <p>Draft § 7155(c).</p>	<p>No, the DPA requirements apply to activities created or generated after July 1, 2023 and are not retroactive. However, a new processing activity is generated when changes to existing activities result in a material changes to the level of risk presented, in which case a DPA may be required.</p> <p>C.R.S. § 6-1-1309(6); Rule 8.05(D), (F).</p>	<p>New DPIAs are not required for processing operations initiated before the GDPR's effective date, but (1) the Article 29 Working Party Guidelines recommends carrying out DPIAs for all high risk operations prior to that date, and (2) a DPIA may have to be conducted or updated where there is a change in the processing activity or risk, as set out in Art. 35.</p>	<p>California's rule is stricter than Colorado's, requiring assessments for ongoing operations at the time of the effective date. Colorado, in contrast, requires assessments only for new activities. Both regimes are still subject to their respective obligation to update assessments (or conduct one in the first instance) in response to changes to processing operations or the risks of harm.</p>
Can one assessment cover multiple processing operations?	<p>Yes, a single RA can cover a "comparable set of processing activities" (defined as "a set of similar processing activities that present similar risks to consumers' privacy").</p> <p>Draft § 7156(a).</p>	<p>Yes, a single DPA may address a "comparable set of Processing operations" (defined as "a set of similar Processing operations including similar activities that present heightened risks of similar harm to a Consumer").</p> <p>C.R.S. § 6-1-1309(5); Rule 8.02(D).</p>	<p>Yes, a single assessment may address a set of similar processing operations that present similar high risks.</p> <p>Art. 35(1).</p>	<p>California and Colorado are consistent on this issue.</p>
Can an assessment conducted for the purpose of complying with another jurisdiction's law or regulation satisfy the requirement?	<p>Yes, if it meets all the requirements of this regulation. An insufficient RA can be supplemented to satisfy the regulations.</p> <p>Draft § 7157(b).</p>	<p>Yes, if the assessment is reasonably similar in scope and effect, or if the controller submits that assessment with a supplement that contains any additional information required by CO.</p> <p>Rule 8.02(B).</p>	<p>According to EDPB Guidelines, "The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them." In any case, a DPIA must meet the requirements in Art. 35(7) to be considered valid under the GDPR.</p> <p>EDPB Guidelines on DPIAs, at page 17.</p>	<p>California and Colorado are consistent on this issue.</p>
When, to whom, and in what form must assessments be submitted?	<p>Annual: Businesses have 24 months from the effective date to submit RA materials for the first time. Subsequent RA materials must then be submitted annually, with no gaps in coverage. RA materials subject to the annual requirement include a signed certification of compliance and an abridged risk assessment. The certification must be signed by a "designated executive" who is the</p>	<p>On Request: Controllers must make DPAs available to AG within 30 days of request.</p> <p>Rule 8.06.</p>	<p>DPIAs are not required to be published, but EDPB Guidelines suggest publishing at least parts (e.g., summary or conclusion) to foster trust and demonstrate compliance. Supervisory authorities may review DPIAs as part of their Art. 58 powers.</p> <p>Recital 89; EDPB Guidelines on DPIAs, at page 18.</p>	<p>Both regimes require a business / controller to submit an assessment to the Attorney General upon request. California's deadline for doing so is shorter than Colorado's—10 days as opposed to 30 days.</p> <p>California differs in requiring that abridged versions of assessments be submitted annually. In prior CPPA board meetings, board</p>

<div>  <div>Comparison of Risk Assessment Requirements: California, Colorado & European Union</div> </div>				
	CCPA Draft Regulations	Colorado Privacy Act Regulations	General Data Protection Regulation	FPF Analysis - California v. Colorado
	<p>highest-ranking executive responsible for oversight of the business's risk assessment compliance. The abridged risk assessment (which can be new or an updated assessment from a prior year) must include: identification of the covered processing activity; a plain language explanation of its purpose for processing PI; categories of PI processed (and whether they include SPI); and a plain language explanation of safeguards implemented or planned to be implemented. Businesses can include a hyperlink to a public webpage containing an unabridged RA. Submissions of RA materials are made via the CPPA website.</p> <p>On Request: Businesses must make unabridged RAs available to CPPA or AG upon request (10 business days).</p> <p>Draft § 7157.</p>			<p>members have stated that mandatory submission of abridged assessments will provide the Agency with a valuable opportunity to learn about business practices and amend regulations as necessary.</p> <p>Absent from California's draft regulations are protections against public records requests and waiver of attorney-client privilege or work-product protections. See Colo. Rev. Stat. § 6-1-1309(4). Failing to provide protections like those in the Colorado Privacy Act could result in businesses producing assessments that are less candid.</p>
Are there additional requirements regarding AI, ADMT, or Profiling?	<p>RA Triggers: There are two categories of processing activities involving ADMT that require RAs—</p> <ul style="list-style-type: none"> • (b)(3): Using of ADMT to make a significant decision or for extensive profiling; and • (b)(4): Processing PI to train ADMT or AI that can be used for making a significant decision, establishing individual identity, physical or biological identification or profiling, deepfake generation, or the operation of generative models. <p>Opt-Out: Although not within scope of this chart, the draft regulations also include rights of notice, access, and opt-out with respect to certain uses of ADMT and AI.</p> <p>Developer Disclosures: For ADMT and AI trained using PI:</p> <ul style="list-style-type: none"> • A business that makes ADMT or AI available to another business for any processing activity that would trigger a RA must provide all facts necessary for the recipient to conduct its own RA. • A business that trains ADMT or AI as set forth in (b)(4), if the business plans to make such ADMT or AI available to another person, must provide a plain language explanation of requirements or limitations the business identified relevant to the permitted use of ADMT or AI. 	<p>DPA Triggers: Profiling requires a DPA if it presents a reasonably foreseeable risk of:</p> <ol style="list-style-type: none"> 1. unfair or deceptive treatment of, or unlawful disparate impact on, consumers; 2. financial or physical injury to consumers; 3. physical or other intrusion upon the solitude/seclusion or private affairs/concerns of consumers if it would be offensive to a reasonable person; 4. or other substantial injury to consumers. <p>Rule 9.06(A). For profiling-specific DPA requirements, see below.</p> <p>Opt-out: Although not within scope of this chart, the regulations also include opt-out rights with respect to profiling in furtherance of decisions that produce legal or other similarly significant effects concerning a consumer. This does not align 1:1 with the types of profiling that require a DPA.</p> <p>Standalone AI Law: In 2024, Colorado enacted a law regulating development and deployment of high-risk AI systems that make or are a substantial factor in making consequential decisions affecting individuals. That law includes impact assessment requirements. That law is outside the scope of this comparison chart. For more information, see FPF's Policy Brief on the Colorado AI Act.</p>	<p>ADMT under the GDPR is generally beyond the scope of this chart. For a detailed overview of the subject, see FPF's prior report on Automated Decision-Making Under the GDPR.</p> <p>DPIA Triggers: Evaluations and decisions that are based on automated decisionmaking with legal or similar effects, including profiling, and forms of evaluation or scoring are singled-out as examples of processing activities likely to result in high risks to fundamental rights and freedoms of individuals.</p> <p>Transparency Requirements: Use of ADMT triggers certain transparency requirements, such as informing data subjects about the existence of and logic involved in ADMT used and explaining the significance and envisaged consequences to the data subject, and opt-out/contestability rights.</p> <p>Art. 35(3); Recital 71; EDPB Guidelines on DPIAs, at pages 8-9; EDPB Guidelines on Profiling, at page 27.</p> <p>EU AI Act: Although outside the scope of this comparison chart, it is important to note that the EU AI Act also requires that certain deployers must, before deploying a high-risk AI system identified in EU AI Act Art. 6(2), perform a fundamental rights impact assessment (FRIA).</p> <p>EU AI Act, Art. 27: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689</p>	<p>California and Colorado use different terms. California refers to ADMT, which includes profiling, whereas Colorado refers to profiling.</p> <p>Both regimes have specific opt-out rights and transparency requirements for use of ADMT / profiling.</p> <p>California and Colorado differ as to when use of ADMT / Profiling triggers an assessment. See that analysis above under "Are there specific processing operations that meet the risk/harm threshold?"</p>
What additional elements must an assessment include for AI / ADMT / Profiling?	<p>Requirements for covered uses of ADMT are divided by the type of use ((b)(3) & (b)(4), see above). For all covered uses of ADMT that trigger a RA, additional requirements include identifying the actions taken or planned to be taken to <i>maintain the quality of PI processed by the ADMT or AI</i> (rule defines quality of PI and provides examples of actions to take).</p> <p>For (b)(3) uses of ADMT, additional requirements include:</p> <ul style="list-style-type: none"> • In identifying operational elements of 	<p>DPA's for profiling must include the elements required under Rule 8.04 as well as the following profiling-specific elements:</p> <ol style="list-style-type: none"> (1) Types of PD used in the profiling; (2) The decision to be made using profiling; (3) Benefits of automated processing over manual processing; (4) Plain language explanation of why the profiling directly and reasonably relates to the controller's goods and services; (5) Explanation of the training data and logic used to create the profiling system; 	<p>Controllers should look to other GDPR provisions concerning ADMT and transparency (e.g., Arts. 13, 14, & 22) when evaluating risks and safeguards in a DPIA.</p> <p>EDPB Guidelines on DPIAs, at page 27.</p> <p>EU AI Act: As mentioned above, the EU AI Act includes an FRIA requirement for certain deployers of high-risk AI systems.</p> <p>EU AI Act, Art. 27.</p>	<p>Colorado has more detailed requirements, including an explanation of fairness and disparate impact testing among other explanations. California introduces a novel requirement to explain how a business maintains the "quality of personal information" processed, which "includes completeness, representativeness, timeliness, validity, accuracy, consistency; and reliability of the sources of the personal information for the business's proposed use of the automated decisionmaking technology or artificial intelligence."</p>

<div>  <div> <div>Comparison of Risk Assessment Requirements: California, Colorado & European Union</div> </div> </div>				
	CCPA Draft Regulations	Colorado Privacy Act Regulations	General Data Protection Regulation	FPF Analysis - California v. Colorado
	<p>processing, identify the logic of the ADMT, assumptions or limitations of the logic, output of the ADMT, and how the business will use the output;</p> <ul style="list-style-type: none"> • In identifying safeguards to mitigate negative impacts to consumers' privacy, identify— <ul style="list-style-type: none"> (i) the whether the business evaluated the ADMT to ensure it works as intended for the proposed use and does not discriminate based upon protected classes; (ii) policies, procedures and training implemented or planned to be implemented to ensure the ADMT works as intended for the proposed use and does not discriminate; and (iii) if the ADMT was obtained from another person, whether the business reviewed that person's evaluation, whether that person's evaluation included requirements or limitations relevant to the proposed use, and any accuracy and nondiscrimination safeguards implemented or planned to implement. <p>Draft § 7152.</p>	<p>(6) Information about purchased third-party software used;</p> <p>(7) Plain language description of outputs;</p> <p>(8) Plain language description of how the outputs will be used, including use for consequential decisions;</p> <p>(9) Information about the degree of human involvement;</p> <p>(10) How the profiling system is evaluated for fairness and disparate impact (and the results of evaluations);</p> <p>(11) Safeguards used to reduce the risks of harms identified;</p> <p>(12) Safeguards for data sets produced by/derived from profiling.</p> <p>Rule 9.06.</p>		

Drafted by Jordan Francis, Policy Counsel for U.S. Legislation at the Future of Privacy Forum (jfrancis@fpf.org)

Note: This chart was prepared based on the California Privacy Protection Agency's (CPPA) draft regulations released for public discussion in advance of the agency's November 8, 2024 board meeting.