NOTE: The Agency has not yet started the formal rulemaking process. The draft text in this document is to facilitate Board discussion and public participation and is subject to change.

DRAFT
INITIAL STATEMENT OF REASONS

JULY 2024

CALIFORNIA PRIVACY PROTECTION AGENCY

TITLE 11. LAW
DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY
CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

INITIAL STATEMENT OF REASONS

PROBLEM STATEMENT

In November 2020, voters approved the California Privacy Rights Act of 2020 ("CPRA"), amending and building on the California Consumer Privacy Act of 2018 ("CCPA"). The CPRA established a new agency, the California Privacy Protection Agency (Agency), to implement and enforce the CCPA. (Civ. Code, § 1798.199.10.)[1] The Agency is directed to adopt regulations to further the purposes of the Act, including promulgating regulations on 22 specific topics. (§ 1798.185.) The proposed regulations do the following things: (1) update existing CCPA regulations; (2) clarify when insurance companies must comply with the CCPA; (3) operationalize requirements to complete an annual cybersecurity audit; (4) operationalize requirements to conduct a risk assessment; and (5) operationalize consumers' rights to access and to opt-out of businesses' use of automated decisionmaking technology.

More specifically, the proposed regulations:

- Add a category to the definition of sensitive personal information. (§ 1798.185, subd. (a)(1).)
- Update rules and procedures that facilitate and govern the submission of a request to opt-out of sale/sharing and a request to limit, and to govern a business's compliance with a consumer's request. (§ 1798.185, subd. (a)(4).)
- Adjust monetary thresholds within the CCPA to reflect increases in the Consumer Price Index. (§ 1798.185, subd. (a)(5).)
- Update rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide under the

[1] All references are to the Civil Code unless otherwise indicated.

CCPA are provided in a manner that may be easily understood by the average consumer. (§ 1798.185, subd. (a)(6).)

- Update rules and procedures to facilitate a consumer's or authorized agent's ability to delete, correct, or obtain personal information. (§ 1798.185, subds. (a)(7), (8), and (9).)
- Clarify regulations defining business purposes for which service providers and contractors may use and combine consumers' personal information. (§ 1798.185, subd. (a)(10).)
- Establish when businesses are to perform a cybersecurity audit, the scope of the audit, and the process to ensure that audits are thorough and independent. (§ 1798.185, subd. (a)(15)(A).)
- Establish when businesses are to conduct a risk assessment with respect to their processing of personal information, what must be included in the risk assessment, the consequence of the risk assessment, and how risk assessments are to be submitted to the Agency. (§ 1798.185, subd. (a)(15)(B).)
- Govern access and opt-out rights with respect to businesses' use of automated decisionmaking technology. (§ 1798.185, subd. (a)(16).)
- Clarify the circumstances under which insurance companies are to comply with the CCPA. (§ 1798.185, subd. (a)(21).)
- Update regulations governing the use or disclosure of a consumer's sensitive personal information. (§ 1798.185, subd. (a)(19)(C).)
- Harmonize regulations governing opt-out mechanisms, notices, and other operational mechanisms to promote clarity and functionality. (§ 1798.185, subd. (a)(22).)
- Further the purposes of the CCPA. (§ 1798.185, subd. (b).)

BENEFITS ANTICIPATED FROM REGULATORY ACTION

This section will be added after completing the Department of Finance review process.

SPECIFIC PURPOSE AND NECESSITY OF EACH SECTION

ARTICLE 1. GENERAL PROVISIONS

§ 7001. Definitions.

Subsection (c) defines "artificial intelligence" to mean a machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments. It also explains that artificial intelligence may do this to achieve explicit or implicit objectives, and the different outputs, autonomy, and adaptiveness after deployment that artificial intelligence may have. Lastly, the definition provides examples of different types of artificial intelligence, such as generative models, facial- or speech-recognition technology, or facial- or speech-detection technology.

This definition is necessary because Article 10's risk-assessment requirements and Article 11's automated decisionmaking technology requirements apply when a business processes consumers' personal information to train certain types of artificial intelligence. Defining this term clarifies when a business must comply with those risk-assessment requirements when training the types of artificial intelligence set forth in subsection 7152(b)(4). In addition, the definition of "automated decisionmaking technology" or "ADMT" set forth in subsection 7001(f) states that ADMT can be derived from artificial intelligence. Defining "artificial intelligence" clarifies which technologies ADMT can be derived from, and therefore when corresponding ADMT requirements for certain uses of ADMT that are set forth in these regulations apply. This definition is informed by and harmonizes with definitions in other frameworks.[2]

[2] *See, e.g.*, Stuart Russell, Karine Perset & Marko Grobelnik, *Updates to the OECD's Definition of an AI System Explained*, OECD (Nov. 29, 2023), https://oecd.ai/en/wonk/ai-system-definition-update; NAT'L INST. OF STANDARDS & TECH., *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Jan. 2023) [hereinafter NIST AI RMF]; European Parliament Legislative Resolution of 13 March 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 2021/0106(COD)) (2024) [hereinafter EU AI Act] (using the term "AI system"); Exec. Order No. 14110, 88 C.F.R. 75191-75226 (2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

Subsection (f) defines "automated decisionmaking technology" and "ADMT" to mean any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking. **Subsection (f)(1)** explains what "technology" includes for the purposes of this definition. **Subsection (f)(2)** explains that "substantially facilitate human decisionmaking" means using the output of the technology as a key factor in a human's decisionmaking and provides an example of using a score as a primary factor to make a significant decision. **Subsection (f)(3)** explicitly clarifies that ADMT includes profiling. Lastly, **subsection (f)(4)** states that ADMT does not include various types of technologies, provided that the business does not use them to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking, or otherwise use them to circumvent the requirements for ADMT in these regulations. It also provides two illustrative examples: one where a business is using a spreadsheet as an ADMT that replaces human decisionmaking, and one where the business is not using a spreadsheet as ADMT.

Subsection (f) is necessary because Civil Code 1798.185, subdivision (a)(16) directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT but does not define this term. This definition addresses the critical role that ADMT can play in human decisionmaking, both by wholly replacing human decisionmaking and by substantially facilitating that decisionmaking. It is necessary to include both of these roles to address harms to consumers' privacy that can result when human decisionmakers significantly rely upon automated decisionmaking technologies in their decisionmaking. For this reason, Agency finds it necessary to clarify that significant reliance on this technology by humans to make a given decision is within scope of the law, which also ensures that consumers enjoy the full protections and benefits of their opt-out and access rights enacted by the CCPA. It also is necessary to avoid any confusion that may result from different understandings of this term. This definition is informed by other frameworks addressing the use of ADMTs.[3]

---

[3] *See, e.g.*, BLUEPRINT FOR AN AI BILL OF RIGHTS MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE, THE WHITE HOUSE (OCT. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [hereinafter BLUEPRINT FOR AN AI BILL OF RIGHTS] (using the term "automated system"); *The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees*, EEOC (May 2022), https://www.eeoc.

Subsection (f)(1) is necessary to provide clarity and guidance for businesses regarding what constitutes a "technology." Because technologies are evolving, the examples in this subsection are illustrative and non-exhaustive. In the Agency's expertise, these examples illustrate the common technologies used as ADMT. **Subsection (f)(2)** clarifies how a technology can be used to "substantially facilitate human decisionmaking." This is necessary to clarify the scope of this term, and more broadly, the scope of the definition of ADMT. As explained above, the Agency recognizes that automated technology can still be "decisionmaking" when it serves as a key factor in a human's decision, because the technology is playing a significant role in driving the decision. It is therefore necessary to clarify the scope of the definition by specifying what it means for an automated technology to "substantially facilitate human decisionmaking." The example provides additional clarity by describing a hypothetical situation in which a human relies on an automated technology to substantially facilitate their decision. **Subsection (f)(3)** is necessary to implement the CCPA's statutory direction in Civil Code section 1798.185, subdivision (a)(16) that ADMT includes profiling and clarifies how these terms work together for businesses. Lastly, **subsection (f)(4)** is necessary to clarify which technologies are excluded from the definition of ADMT. As long as such technologies are not used to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking, these common computational programs are generally excluded from the scope of the ADMT definition. This subsection is also necessary to provide clarity and guidance for businesses and consumers regarding when technologies fall in and out of scope of the ADMT definition and to clarify that these technologies may not be used to circumvent the requirements for ADMT.

Subsection (g) defines "behavioral advertising" to mean the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity. It establishes that this includes a consumer's activity across businesses, distinctly-branded websites, applications, or services, or within the business's own distinctly-branded websites, applications, or services. **Subsection (g)(1)** explains that behavioral advertising includes cross-context behavioral advertising. **Subsection (g)(2)** explains that behavioral advertising does

---

gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence [hereinafter EEOC Job Applicant and Employee Guidance] (using the term "algorithmic decision-making tools"); Rashida Richardson, *Definitions and Demystifying Automated Decision Systems*, 81 MARYLAND L. REV. 785 (2022) (using the term "automated decision system").

not include nonpersonalized advertising, which is defined in Civil Code section 1798.140, subdivision (t), provided that the consumer's personal information is not used to build a profile about them or otherwise alter their experience outside their current interaction with the business and is not disclosed to a third party.

Subsection (g) is necessary because certain risk-assessment and ADMT requirements apply to the use of ADMT for profiling for behavioral advertising. The term behavioral advertising by itself is not defined by the CCPA. This definition draws from the CCPA's definition of "cross-context behavioral advertising" for consistency and clarifies that behavioral advertising means any targeting of advertising to a consumer based on their personal information obtained from the consumer's activity. **Subsection (g)(1)** is necessary to clarify that cross-context behavioral advertising is one type of behavioral advertising. **Subsection (g)(2)** is necessary to clarify that nonpersonalized advertising, as defined by the CCPA, is excluded from the scope of behavioral advertising; and how to qualify for that exclusion (e.g., the consumer's personal information must not be disclosed to a third party). This is also consistent with how nonpersonalized advertising is treated under Civil Code section 1798.140, subdivision (e)(4).

Subsection (*l*) defines "cybersecurity audit" to mean the annual cybersecurity audit that every business must complete if their processing of consumer's personal information presents significant risk to consumers' security, as set forth in subsection 7120(b). This definition is necessary to provide clarity and guidance regarding the term "cybersecurity audit," which is used repeatedly throughout these regulations and is what is required by the CCPA (Civ. Code, § 1798.185, subd. (a)(15(A)) if a business meets one of the thresholds set forth in subsection 7120(b). It also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (m) defines "cybersecurity program" to mean the policies, procedures, and practices that protect personal information from unauthorized access, destruction, use, modification, or disclosure; and protect against unauthorized activity resulting in the loss of availability of personal information. This definition is necessary to provide clarity and guidance regarding the term "cybersecurity program," which is used repeatedly throughout these regulations. This definition is informed by and harmonizes with definitions and descriptions of privacy and information security programs, and cybersecurity programs and policies in other

contexts.[4] It also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (n) defines "deepfake" to mean manipulated or synthetic audio, image, or video content that depicts a consumer saying or doing things they did not say or do and that are presented as truthful or authentic without the consumer's knowledge or permission. This definition is necessary because certain risk-assessment and ADMT requirements apply to the training of artificial intelligence ("AI") or ADMT that is capable of being used to generate deepfakes. This definition is informed by and harmonizes with others' definitions of "deepfake."[5]

Subsection (v) defines "information system" to mean the resources organized for the processing of information. It provides examples of resources, such as network, hardware, and software. It also provides examples of different types of processing, such as the collection, use, disclosure, sale, sharing, and retention of personal information. This definition is necessary to provide clarity and guidance regarding the term "information system," which is used repeatedly throughout these regulations. It is informed by and harmonizes with others' definitions of this term, such as those from the National Institute of Standards and Technology ("NIST") and the New York State Department of Financial Services ("NYDFS").[6] It also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (w) defines "multi-factor authentication" to mean authentication through verification of at least two of the following types of authentication factors:

---

[4] *See, e.g.,* Standards for Safeguarding Customer Information, 16 C.F.R. § 314.3 (using the term "comprehensive information security program"); N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.2(a)–(b), 500.3; Final Decision and Order at 4, Blackbaud, Inc., No. C-4804 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2023181_blackbaud_final_consent_package.pdf (using the term "Information Security Program"); Final Decision and Order at 9, BetterHelp, Inc., FTC Docket No. C-4796 (July 14, 2023) https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpfinalorder.pdf (using the term "Privacy Program").

[5] *See, e.g.*, *Science & Tech Spotlight: Deepfakes*, U.S. GOV'T ACCOUNTABILITY OFFICE (Feb. 2020), https://www.gao.gov/assets/gao-20-379sp.pdf; Meredith Somers, *Deepfakes, Explained*, MIT MGMT. SLOAN SCH. (July 21, 2020), https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.

[6] *See, e.g.*, NAT'L INST. OF STANDARDS & TECH., FIPS PUB 200, Federal Information Processing Standards Publication, MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS (Mar. 2006), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf; 44 U.S.C. § 3502(8); N.Y. COMP. CODES R. & REGS. tit. 23, § 500.1(i).

(1) knowledge factors; (2) possession factors; and (3) inherence factors. It also provides an example of each factor. This definition is necessary to clarify what constitutes multi-factor authentication, because multi-factor authentication is a component of a cybersecurity program that the business's cybersecurity audit must specifically identify, assess, and document, as applicable. This definition provides clarity about what multi-factor authentication requires and is informed by and harmonizes with others' definitions of this term, such as those from the Federal Trade Commission ("FTC") and the NYDFS.[7]

Subsection (x) has been revised to add "many" before non-profits because the definition of business includes non-profits that control or are controlled by a business that shares common branding with the business and with whom the business shares consumer personal information. (*See* Civ. Code, § 1798.140, subd. (d)(2).) Corresponding grammatical changes have been made to the example to reflect this. These changes are necessary to align the regulation with the language of the statute and to clear up any confusion on this issue.

Subsection (dd) defines "penetration testing" to mean testing the security of an information system by attempting to circumvent or defeat its security features by authorizing attempted penetration of the information system. This definition is necessary to clarify what constitutes penetration testing, because penetration testing is a component of a cybersecurity program that the business's cybersecurity audit must specifically identify, assess, and document, as applicable. This definition provides clarity about what penetration testing requires and is informed by others' definitions and descriptions of this term, such as those from the FTC and NYDFS.[8]

---

[7] *See, e.g.,* Standards for Safeguarding Customer Information, 16 C.F.R. § 314.2(k); N.Y. COMP. CODES R. & REGS. tit. 23, § 500.1(j); NAT'L INST. OF STANDARDS & TECH., SP 1800-12A, DERIVED PERSONAL IDENTITY VERIFICATION (PIV) CREDENTIALS (Aug. 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-12.pdf; FED. TRADE COMM'N, *FTC Safeguards Rule: What Your Business Needs to Know* (May 2022), https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know.

[8] *See, e.g.,* FED. TRADE COMM'N, Standards for Safeguarding Customer Information, 16 C.F.R. § 314.2(m); N.Y. COMP. CODES R. & REGS. tit. 23, § 500.1(*l*); NAT'L INST. OF STANDARDS & TECH., NIST SP 800-53, REV. 5, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf; FED. TRADE COMM'N, *FTC Safeguards Rule: What Your Business Needs to Know* (May 2022), https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know.

Subsection (ee) defines "performance at work" to mean the performance of job duties for which the consumer has been hired or has applied to be hired. It also provides a list of items that do not meet this definition: a consumer's union membership or interest in unionizing; a consumer's interest in seeking other employment opportunities; a consumer's location when off-duty or on breaks; or a consumer's use of a personal account, unless solely to prevent or limit the use of these accounts on the business's information system or to prevent the disclosure of confidential information.

This definition is necessary to clarify when evaluating or analyzing a consumer's performance at work constitutes profiling, because certain risk-assessments and ADMT requirements may attach when a business is profiling a consumer. In addition, certain exceptions to a business's requirement to provide the ability to opt-out of ADMT also requires assessment of whether the ADMT is necessary to achieve, and is used solely for, an assessment of the consumer's performance at work. (*See* subsections 7221(b)(3)(A), (5)(A).) Accordingly, it is necessary to clarify what performance at work entails to avoid confusion about what falls within scope of this exception. Lastly, the definition's list of excluded items (e.g., a consumer's union membership) is necessary to clarify that a business cannot rely on the exceptions in subsections 7221(b)(3)(A) or (5)(A) if it is using ADMT to profile a consumer to analyze or evaluate their union membership or interest in union membership, their interest in seeking other employment opportunities, their location outside of their job duties, or certain uses of their personal accounts. This list avoids potential overuse of the exceptions in subsections 7221(b)(3)(A) and (5)(A) for non-job activities.

Subsection (ff) defines "performance in an educational program" to mean the performance of coursework in an educational program in which the consumer is enrolled or has applied to be enrolled. It also provides a list of items that do not meet this definition: a consumer's use of a personal account, unless solely to prevent or limit the use of these accounts on the educational program provider's information system, including to prevent the disclosure of confidential information or to prevent cheating; or a consumer's location when they are not performing coursework.

This definition is necessary because certain exceptions to a business's requirement to provide the ability to opt-out of ADMT also requires assessment of whether the ADMT is necessary to achieve, and is used solely for, an assessment of the

consumer's performance in an educational program. (*See* subsections 7221(b)(3)(A), (b)(5)(A).) It is necessary to clarify what performance in an educational program entails to avoid confusion about what falls within scope of this exception. Lastly, the definition's list of excluded items (e.g., a consumer's location when they are not performing coursework) is necessary to clarify that a business cannot rely on the exceptions in subsections 7221(b)(3)(A) and(b)(5)(A) if it is using ADMT to profile a consumer to evaluate or analyze their location when they are not performing coursework or certain uses of their personal accounts. This list avoids potential overuse of the exceptions in subsections 7221(b)(3)(A) and (b)(5)(A) for non-educational activities.

Subsection (gg) defines "physical or biological identification or profiling" to mean identifying or profiling a consumer using information that depicts or describes their physical or biological characteristics, or measurements of or relating to their body. It also establishes that this includes using biometric information, vocal intonation, facial expression, and gesture.

This definition is necessary because risk-assessment and ADMT requirements apply to certain uses of physical or biological identification or profiling, including the training of AI or ADMT that is capable of being used for physical or biological identification or profiling. This definition clarifies what constitutes "physical or biological identification or profiling" to avoid confusion about what is in scope of the term and therefore when the risk-assessment and ADMT requirements apply. It is informed by principles in a recent proposed order from the FTC.[9]

Subsection (jj) defines "privileged account" to mean any authorized user account or service account that can be used to perform functions that other user accounts are not authorized to perform, including but not limited to the ability to add, change, or remove other accounts, or make configuration changes to an information system. It also explains what constitutes an authorized user account or service account.

This definition is necessary because account management and access controls for privileged accounts is a component of a cybersecurity program that the business's cybersecurity audit must specifically identify, assess, and document, as applicable. This definition provides clarity about what privileged accounts are and is informed

[9] *See, e.g., FTC v. Rite Aid Corp.*, No. 2:23-cv-6023, Exhibit A: Proposed Stipulated Order for Permanent Injunction and Other Relief (Dec. 19, 2023).

by others' definitions and descriptions of this term, such as those from the NIST and the NYDFS.[10]

Subsection (kk) defines "profiling" to mean any form of automated processing of personal information to evaluate certain natural aspects relating to a natural person and, in particular, to analyze or predict aspects concerning the natural person's intelligence, ability, aptitude, performance at work, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements.

This definition is necessary because several risk-assessment and ADMT requirements apply when a business uses ADMT for certain types of profiling (e.g., public profiling). It is necessary to clarify what types of profiling are in scope of these requirements. It is also necessary because the CCPA directs the Agency to further define the statutory definition of profiling. To implement the CCPA's statutory requirement that the Agency further define "profiling," the proposed regulation further defines "profiling" to include analyzing or predicting aspects concerning a natural person's intelligence, ability, aptitude, and predispositions, and make explicit that health includes mental health. These additions are consistent with how the CCPA addresses the creation of profiles of consumers reflecting these aspects in the definition of "personal information." (*See* Civ. Code § 1798.140, subd. (v)(1)(K).) Lastly, the entire definition of profiling has been included to make the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (*ll*) defines "publicly accessible place" to mean a place that is open to or serves the public. It also provides a non-exhaustive list of examples of publicly accessible places. This definition is necessary because several risk-assessment and ADMT requirements apply when a business uses ADMT to profile a consumer through systematic observation of a publicly accessible place. Defining the term "publicly accessible place" clarifies which places are in scope of these requirements. It is consistent with common understandings of publicly accessible

[10] *See, e.g.,* NAT'L INST. OF STANDARDS & TECH., NIST SP 800-53, Rev. 5, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf; N.Y. COMP. CODES R. & REGS. tit. 23, § 500.1(n).

places where profiling a consumer through systematic observation poses significant risk to their privacy.

Subsection (mm) defines "request to access ADMT" to mean a consumer request that a business provide information to the consumer about the business's use of ADMT with respect to the consumer, pursuant to Civil Code section 1798.185, subdivision (a)(16) and Article 11 of these regulations. The definition is necessary to clearly identify and avoid any confusion regarding which requests the regulations are referring to when setting forth the rules and procedures businesses must follow for requests to access ADMT. It allows the regulations to group together the requirements businesses must follow in responding to requests to access ADMT. It also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (nn) defines "request to appeal ADMT" to mean a consumer request to appeal the business's use of ADMT for a significant decision as set forth in subsection 7221(b)(2). This definition is necessary to clarify which requests to appeal the regulations are referring to when setting forth the rules and procedures businesses must follow to qualify for the appeal exception to the opt-out of ADMT requirements. The use of the shortened phrase "request to appeal ADMT" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (qq)(4), (5), and (6) have been revised to add "shared" and "sharing" to the categories of personal information, as well as the purposes, that can be requested by consumers as part of a request to know. These changes have been made to align the regulation to the amended language of the statute. (*See* Civ. Code, §§ 1798.110, 1798.115.) **Subsection (z)(5)** has also been revised to delete "for a business purpose" because third parties are persons to whom personal information is sold or shared, not disclosed for a business purpose. (*Id.*, § 1798.140, subd. (ai).) This change is necessary to align the regulation with the language of the statute.

Subsection (tt) defines "request to opt-out of ADMT" to mean a consumer request that a business not use ADMT with respect to the consumer, pursuant to Civil Code section 1798.185, subdivision (a)(16) and Article 11 of these regulations. The definition is necessary to clearly identify and avoid any confusion regarding which requests the regulations are referring to when setting forth the rules and procedures businesses must follow for requests to opt-out of ADMT. It allows the

regulations to group together the requirements businesses must follow in responding to requests to opt-out of ADMT. It also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (vv) defines "right to access ADMT" to mean a consumer's right to request that a business provide information to the consumer about the business's use of ADMT with respect to the consumer as set forth in Civil Code section 1798.185, subdivision (a)(16) and Article 11 of these regulations. This definition is necessary to clarify what this term refers to when it is used in the regulations. The use of the shortened phrase "right to access ADMT" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (aaa) defines "right to opt-out of ADMT" to mean a consumer's right to direct that a business not use ADMT with respect to the consumer as set forth in Civil Code section 1798.185, subdivision (a)(16) and Article 11 of these regulations. This definition is necessary to clarify what this term refers to when it is used in the regulations. The use of the shortened phrase "right to opt-out of ADMT" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (ccc) has been added to expand the statutory definition of sensitive personal information to include the personal information of consumers whom the business has actual knowledge are less than 16 years of age. Civil Code sections 1798.185, subdivision (a)(1), and 1798.199.40, subdivision (b), give the Agency authority to update and add categories to the definition of sensitive personal information to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns. Civil Code section 1798.199.40, subdivision (i), also tasks the Agency to work with other jurisdictions to ensure consistent application of privacy protections.

Adding the personal information of consumers known to be less than 16 years of age to the definition of sensitive personal information does two things. First, it harmonizes California's definition with the definition of sensitive data used by other jurisdictions (e.g., Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, and Virginia), which include within their definition of sensitive data language such as: "personal data of a known child," "personal data collected from a known child," or "a child's personal data." "Child" in their laws is defined to be a person less than 13 years of age.

Second, the definition reflects how California's law gives additional protections to consumers 13 to 15 years of age, unlike most of these other jurisdictions. Civil Code section 1798.120, subdivisions (c) and (d), prohibits businesses from selling or sharing the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer or their parent or guardian (for those less than 13 years of age) affirmatively authorized it. Including the personal information of consumers less than 16 years of age in the definition of sensitive personal information gives consumers under the age of 16 years of age the ability to direct businesses to only use their personal information to perform the services or provide the goods that they would reasonably expect, and for the limited purposes prescribed by the CCPA.

The rest of the definition of sensitive personal information is a reiteration of Civil Code section 1798.140, subdivision (ae), and is included for readability and ease of reference. This regulation benefits businesses and consumers by providing consistency in the terms used by other jurisdictions, while also addressing the additional protections provided by the CCPA.

Subsection (eee) defines "systematic observation" to mean methodical and regular or continuous observation. It also provides examples of different technologies that can enable methodical and regular or continuous observation. This definition is necessary because several risk-assessment and ADMT requirements apply when a business uses ADMT to profile a consumer in certain ways through systematic observation. Defining "systematic observation" clarifies which types of profiling are in scope of these requirements. This definition is informed by the plain language definitions of the term "systematic."

Subsection (fff) explains that "train automated decisionmaking technology or artificial intelligence" means the process through which ADMT or AI discovers underlying patterns, learns a series of actions, or is taught to generate a desired output. It provides a non-exhaustive list of examples of training. This definition is necessary because several risk-assessment and ADMT requirements apply to processing consumers' personal information to train certain ADMT or AI. Defining the term "train automated decisionmaking technology or artificial intelligence" clarifies what training these technologies means and therefore what processing of consumers' personal information are in scope of these requirements. This definition

is informed by approaches taken by other agencies and regulators, such as the NIST and the Commission Nationale de L'informatique et des Libertés.[11]

Subsection (jjj) has been revised to add "request to access ADMT." This revision is necessary because subsection 7222(d) requires that businesses verify the identity of the person making the request to access ADMT as set forth in Article 5. This revision is necessary to ensure consistency throughout the regulations and make clear that the verification requirements in Article 5 apply to requests to access ADMT.

Subsection (kkk) defines "zero trust architecture" to mean denying access to an information system and the information that it processes by default, and instead explicitly granting and enforcing only the minimal access required. It explains that zero trust architecture is based upon the acknowledgement that threats exist both inside and outside the business's information system, and it avoids granting access based upon any one attribute. It also provides an example of how an information system would use zero trust architecture.

This definition is necessary because zero trust architecture is a component of a cybersecurity program that the business's cybersecurity audit must specifically identify, assess, and document, as applicable. This definition provides clarity about what zero trust architecture is and is informed by others' definitions and descriptions of this term, such as those from the President's Executive Order on Improving the Nation's Cybersecurity and NIST.[12]

---

[11] *See, e.g.*, TRUSTWORTHY & RESPONSIBLE AI RES. CTR., NAT'L INST. OF STANDARDS & TECH., THE LANGUAGE OF TRUSTWORTHY AI: AN IN-DEPTH GLOSSARY OF TERMS (updated May 13, 2024), https://docs.google.com/spreadsheets/d/e/2PACX-1vTRBYglcOtgaMrdF11aFxfEY3EmB31zslYI4q2_7ZZ8z_1lKm7OHtF0t4xIsckuogNZ3hRZAaDQuv_K/pubhtml (definition of "model training"); *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, EUROPEAN PARLIAMENTARY RESEARCH SERVICE (June 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf; GSA, *AI Guide for Government – Understanding and Managing the AI Lifecycle*, https://coe.gsa.gov/coe/ai-guide-for-government/understanding-managing-ai-lifecycle/index.html; Commission Nationale de L'informatique et des Libertés, *AI: Ensuring GDPR Compliance* (Sept. 21, 2022), https://www.cnil.fr/en/ai-ensuring-gdpr-compliance.

[12] *See, e.g.,* Exec. Order No. 14028, 3 C.F.R. 556 (2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; NAT'L INST. OF STANDARDS & TECH., SP 800-160, Vol. 2, Rev. 1, DEVELOPING CYBER-RESILIENT SYSTEMS: A

Changes without regulatory effect. The subsections have been renumbered.

§ 7002. Restrictions on the Collection and Use of Personal Information.

Subsection (c)(2) has been revised to replace "through" with a hyphen. This is a non-substantive change.

Subsection (e) has been revised to add language to clarify that a consumer shall be able to withdraw consent at any time. The revised language notes where some statutory exceptions apply. This change is necessary to clarify that the natural byproduct of consent that is freely given, as required under Civil Code section 1798.140, subdivision (h), is that it can be withdrawn at any time. This is consistent with Civil Code section 1798.125, subdivision (b)(3), which states that consent given to participate in a financial incentive program can be revoked by the consumer at any time. It is also consistent with Colorado regulations.[13] This change benefits businesses by explaining that freely given consent means that it can be withdrawn at any time. It also benefits consumers by making clear that they have the right to withdraw consent at any time.

Subsection (f) has been revised to clarify that a business' collection or processing of personal information shall comply with subsections (a) through(e), not just subsection (a). This is a non-substantive change because subsections (b) through (e) explain in greater detail how to comply with subsection (a).

§ 7003. Requirements for Disclosures and Communications to Consumers.

Subsection (c) has been revised to replace "its homepage(s)" with "any internet webpage where personal information is collected." This is a non-substantive change because "homepage" is defined in the statute to include any internet webpage where personal information is collected. This change is necessary because businesses and consumers may not realize that the statutory definition of "homepage" is broader than how it is commonly used. This change benefits

---

SYSTEMS SECURITY ENGINEERING APPROACH (Dec. 2021), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf; NAT'L INST. OF STANDARDS & TECH., SP 800-207, ZERO TRUST ARCHITECTURE (Aug. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[13] *See* 4 COLO. CODE REGS., § 904-3-7.03 (2023) ("Consent is freely given when Consumers may refuse Consent without detriment and withdraw Consent easily at any time."); *see also* § 904-3-7.07.

businesses by making clear the businesses' obligations under the law when posting a conspicuous link. Consumers will also benefit from the increased compliance by businesses.

Subsection (d) has been revised to replace "may" with "must." The subsection now requires mobile applications to include a conspicuous link within the application itself, such as through the application's settings menu, in addition to being accessible through the mobile application platform or download page. This change is necessary to ensure that businesses make the link easily accessible not only before the consumer downloads the application, but within the application. This change allows consumers who are already using mobile applications to access required information more easily. The change also provides businesses with clear guidance about what is required of them.

§ 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.

Subsection (a) has been revised to strengthen language throughout the subsection to make clear that businesses must incorporate the principles provided in designing and implementing their methods for submitting CCPA requests and for obtaining consumer consent. Examples have also been revised or added to further illustrate these principles and to explain that the examples are often requirements in those factual scenarios. These changes are necessary to clarify what is required of businesses and to address potential confusion regarding the application of these principles. Some examples have also been added to harmonize California requirements with other jurisdictions, like Colorado's requirements for consent. These revisions benefit businesses because they provide clear guidance about how to comply with the law. Consumers benefit because the revisions ensure that their consent is freely given, specific, informed, and is an unambiguous indication of their wishes.

The specific changes are addressed in greater detail below.

- **Subsection (a)(2)** has been revised to add "and requirements" to be more precise. The examples provided illustrate principles that are required under the regulations. This is a non-substantive change.

- **Subsection (a)(2)(A)** has been revised to provide a simpler example that demonstrates the principle that methods for submitting CCPA requests and obtaining consumer consent must provide symmetry in choice.

- **Subsections (a)(2)(D) and (E)** have been added to provide further examples of how choices presented to the consumer would not be symmetrical. They are similar to examples within Colorado's regulations regarding consent. (4 Colo. Code Regs. §§ 904-3-7.09(B)(3), (4), and (7).)

- **Subsection (a)(3)** has been revised to strengthen language throughout the subsections (e.g., changing "avoid" to "do not use" and "should" to "must") to make clear that businesses shall not use language or interactive elements that are confusing. The subsection has also been revised to prohibit businesses from using misleading statements or omissions, affirmative misstatements, or deceptive language in obtaining consent. **Subsections (a)(3)(D) and (E)** have also been added to provide additional examples of how a consumer's silence or failure to act affirmatively does not constitute consent and choices driven by a false sense of urgency are misleading. These changes are consistent with existing law prohibiting unfair and deceptive practices, as well as prohibitions seen in other jurisdictions. (*See* Bus. & Prof. Code §§ 17200, 17500 (West, Westlaw through Ch. 1 of 2022 Reg. Sess.); 4 Colo. Code Regs. § 904-3-7.09(B)(7) (2023).)

- **Subsection (a)(4)** has been revised to strengthen language throughout the subsections (e.g., changing "may" to "must" and "avoid" to "do not use" and adding "requirements").

- **Subsection (a)(4)(C)** was added to provide another example that illustrates how choice architecture can impair a consumer's ability to make a choice. This example is similar to an example in Colorado's regulations regarding consent. (*See* 4 Colo. Code Regs. §§ 904-3-7.03(B)-(D), 7.09(B)(3) (2022).)

- **Subsection (a)(5)** has been revised to make clear that methods must be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request. Language was also added to clarify that this principle also applies to methods for providing and withdrawing consent.

- **Subsection (a)(5)(C)** was expanded to provide additional examples of what could be a violation of the regulation.
- **Subsection (a)(5)(D)** was added to remind businesses that individuals handling phone calls from consumers submitting CCPA requests must have the knowledge and ability to process those requests. This is an example of how methods for submitting CCPA rights and obtain consent must be easy to execute. This addition was based on feedback received from consumers that individuals handling phone calls from consumers submitting CCPA requests did not have the knowledge or ability to do so.

Subsection (b) has been revised to take out unnecessary words and to make clear that the illustrative examples in subsection (a) were a non-exhaustive list of dark patterns.

Subsection (c) has been revised to make clear that a user interface that has the effect of subverting or impairing consumer choice was a dark pattern even if the business did not intend to do so. The last sentence was also deleted as unnecessary.

§ 7005. Consumer Price Index Adjustment.

Civil Code section 1798.185, subdivision (a)(5), requires the Agency to increase monetary thresholds specified in the CCPA in January of every odd-numbered year. The amounts are to increase to reflect any increase in the Consumer Price Index.

Subsection (a) identifies the consumer price index by which the monetary thresholds will increase and explains how any increase would be calculated. This regulation is necessary because there are multiple consumer price indexes and the CCPA does not specify which one to use or how to calculate the increase. The index selected and identified in this regulation is recommended by the California Department of Finance. It is also the index used by the Agency for changes to its annual budget. This regulation benefits businesses and consumers by providing clarity regarding the monetary amounts. It removes any ambiguity to the calculation so that future changes to the monetary thresholds can be made through Section 100 changes.

Subsection (b) identifies each monetary threshold that will adjust with any increase in the Consumer Price Index. This regulation benefits businesses and consumers by

placing all the monetary thresholds in one place to be easily adjusted and accessible to them.

ARTICLE 2. REQUIRED DISCLOSURES TO CONSUMERS

§ 7010. Overview of Required Disclosures.

Subsection (c) has been added to clarify that a business that uses ADMT as set forth in subsection 7200(a), must provide consumers with a Pre-use Notice in accordance with section 7220. This regulation is necessary to align section 7010 with the new required disclosures to consumers under Article 11 regarding consumers' rights to opt-out of and access ADMT. It also makes the regulations more readable because it ensures that businesses have a list of required disclosures in one place, with cross-references to sections 7200 and 7220, if they would like to read the more fulsome requirements for Pre-use Notices.

Subsection (d) has been added to clarify that a business that uses ADMT as set forth in subsection 7200(a), must include in its Pre-use Notice a link through which consumers can opt-out of the business's use of ADMT. This regulation is necessary to align section 7010 with the new required opt-out link for the right to opt-out of ADMT. This subsection includes the language "[e]xcept as set forth in section 7221, subsection (b)(1)" to acknowledge that if a business meets one of the exceptions set forth in that section, it is not required to provide the opt-out link to consumers, because it is not required to provide the ability to opt-out of ADMT. Lastly, this subsection makes the regulations more readable because it ensures that businesses have a list of required disclosures in one place, with a cross-reference to subsection 7221(c)(1) if they would like to read the more fulsome requirements for the opt-out link.

Changes without regulatory effect. The subsections have been renumbered and reference citations have been amended.

§ 7011. Privacy Policy.

Subsection (d) has been revised to replace "may" with "must." This is necessary to provide consumers an easy way to access information about the business's collection and use of personal information within the mobile application. Requiring inclusion of a link to the privacy policy in the application's settings menu is necessary so that a consumer does not have to search for the application's

download page to access the privacy policy. This revision benefits businesses by providing clear direction regarding what is expected of them, and it benefits consumers who are already using mobile applications, enabling them to access the privacy policy more easily.

Subsections (e)(1)(B) and **(E)** have been revised to add language that requires businesses to describe categories of sources and categories of third parties in a manner that provides consumers a meaningful understanding of those things. This language is necessary to ensure that businesses' privacy policies are easy to understand, which will benefit consumers.

Subsection (e)(1)(H) has been revised to use "service provider or contractor" instead of "third parties" because disclosures for a business purpose are made to service providers and contractors, not third parties. This change benefits businesses and consumers because it explains businesses' obligations more precisely.

Subsection (e)(1)(I) has been deleted because it is unnecessary.

Subsection (e)(2)(F) has been added to clarify that businesses must include an explanation of consumers' right to opt-out of ADMT, if they are using ADMT as set forth in subsection 7200(a). It also states "[e]xcept as set forth in section 7221, subsection (b)" to acknowledge that if a business meets one of the exceptions set forth in that section, it is not required to provide this explanation to consumers, because it is not required to provide the ability to opt-out of ADMT. This regulation is necessary to ensure that consumers have an explanation of their CCPA rights, which now includes the right to opt-out of ADMT, in one place in the privacy policy.

Subsection (e)(2)(G) has been added to clarify that a business must provide an explanation of the right to access ADMT if it is using ADMT as set forth in subsections 7200(a)(1)–(2). This regulation is necessary to ensure that consumers have an explanation of their CCPA rights, which now includes the right to access ADMT, in one place in the privacy policy.

Subsection (e)(2)(H) has been revised to clarify that consumers have a right against retaliation when exercising their privacy rights, and that this right also applies when they are acting as an applicant to an educational program, a job applicant, or a student. This revision is necessary to align this subsection with the name of the right set forth in Civil Code section 1798.125 ("Consumers' Right of No Retaliation

Following Opt Out or Exercise of Other Rights"). It also ensures consistency with the disclosure requirements for businesses (i.e., that they inform consumers that they cannot be retaliated against for exercising their rights to opt-out of or access ADMT) set forth in sections 7220 and 7222.

Subsection (e)(3)(E) has been revised to add "request to access ADMT." This revision is necessary because subsection 7222(d) requires that businesses verify the identity of the person making the request to access ADMT as set forth in Article 5. This revision is necessary to ensure consistency throughout the regulations, specifically with how businesses describe their verification requirements for all applicable CCPA rights. It also ensures that consumers have a description of businesses' verification processes for these rights in one place in the privacy policy.

Changes without regulatory effect. Non-substantive changes (e.g., adjustments to punctuation and renumbering of subsections) have been made throughout the section. Reference citations have also been amended.

§ 7012. Notice at Collection of Personal Information.

Changes without regulatory effect. Non-substantive changes (e.g., adjustments to punctuation and deletion of unnecessary words) have been made throughout the section.

§ 7013. Notice of Right to Opt-Out of Sale/Sharing and the "Do Not Sell or Share My Personal Information" Link.

Subsection (e)(3) has been revised to add "and requirements" to be more precise. The examples provided illustrate principles that are required under the regulations. This is a non-substantive change.

Subsections (e)(3)(C) and **(D)** have been added to provide more examples of the requirement that the Notice of Right to Opt-Out of Sale/Sharing be provided in the same manner in which the business collects the personal information that it sells or shares. Specifically, these subsections are necessary to provide examples of how to give the notice when personal information is collected and sold or shared through connected devices or in augmented or virtual reality. They benefit consumers by ensuring that the notice is effective in informing consumers of their right to opt-out of the sale/sharing.

§ 7014. Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" Link.

Subsection (e)(3) has been added to further implement Civil Code section 1798.135, subdivision (a)(2), regarding how to make the notice of right to limit reasonably accessible to consumers. It recognizes that businesses may collect sensitive personal information in many ways, so any notice of the consumer's right to limit the use of that sensitive personal information should be provided in the same manner in which the business collects the sensitive personal information that it uses or discloses for purposes other than those specified in the law. This requirement takes a performance-based approach to adapt notices to the context in which the sensitive personal information is collected and provides four illustrative examples.

Subsection (e)(3) is necessary to facilitate consumer awareness and the effectiveness of the Notice of Right to Limit. The subsection benefits consumers because offering the notice in the same manner in which the consumer's right to limit applies allows the consumer to learn of and exercise their right when it is most relevant to them. The subsection also benefits businesses in that it mirrors the requirements for the Notice of Right to Opt-Out of Sale/Sharing, and thus, eases the implementation burden on businesses.

§ 7015. Alternative Opt-out Link.

Subsection (b) has been revised to include subsections to make the regulation easier to read. This is a non-substantive change. **Subsection (b)(3)** has also been added to ensure that the opt-out icon is conspicuous and easy to read. The subsection is necessary to respond to public comments seeking guidance on how to comply with the regulation when the color of the icon matches the background of a business's website. The subsection focuses on the performative standard of visibility and is not prescriptive to provide businesses flexibility. It benefits businesses by providing requested guidance and benefits consumers by ensuring that the icon is conspicuous and visible.

ARTICLE 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

§ 7020. Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know.

Subsection (e) has been added to require businesses to provide a means by which the consumer can request that the business, in response to a request to know, provide personal information collected prior to the 12-month period preceding the business's receipt of the request. This regulation is necessary because consumers may not know that, upon request, they are entitled to obtain this information. Civil Code section 1798.130, subdivision (a)(2)(B), requires that a business, in response to a request to know, provide the consumer with the personal information that it collected about them within the 12-month period preceding the request. Upon request, a business is obligated to provide information beyond that 12-month period (as far back as January 1, 2022). (Civ. Code, § 1798.130(a)(2)(B); 11 C.C.R. § 7024(h).) Because the onus is on the consumer to make the request, this regulation is necessary to ensure that the consumer has the opportunity to make such a request. It benefits consumers by informing them of their right to access more information and ensures that it is easy for them to fully exercise that right. The regulation also benefits businesses in that it does not prescribe how a business must provide a means by which the consumer can exercise their choice. Instead, the regulation takes a performance-based approach so that businesses have flexibility on how to provide this option.

Changes without regulatory effect. The subsections have been renumbered.

§ 7021. Timelines for Responding to Requests to Delete, Requests to Correct, Requests to Know, and Requests to Access ADMT, and Requests to Appeal ADMT.

Subsections (a) and **(b)** have been revised to include "request to access ADMT" and "request to appeal ADMT." This revision applies existing timelines for responding to other consumer requests to requests to access and appeal ADMT. This change is necessary to operationalize the right to access ADMT and the appeal exception to the right to opt-out of ADMT. By using the same timing requirements, this regulation benefits businesses by enabling them to leverage existing timeline processes for other CCPA rights and extend them to requests to access and appeal ADMT.

§ 7022. Requests to Delete.

Subsection (b) has been revised to make clear that businesses must do all of the following things listed in subsections (b)(1) through (b)(3). This is a non-substantive change.

Subsections (b)(1) and **(c)(1)** have been revised to add language that makes clear that businesses, service providers, and contractors are to implement measures to ensure that information subject to a request to delete remains deleted, deidentified, or aggregated.

Subsection (f) has also been added to explain that whether a business, service provider, or contractor has implemented these measures factors into whether they have complied with the consumer's request to delete. It also explains that a business, service provider, or contractor should consider and address how previously deleted information may be recollected if they receive personal information from data brokers on a regular basis. These obligations are consistent with proposed requirements that businesses implement measures to ensure that personal information subject to a request to correct remain corrected.

These subsections are necessary to address commonly occurring situations related to the collection of personal information and to ensure that a consumer's right to delete is meaningful. Whether someone has adequately complied with a consumer's request to delete is ultimately a fact-specific determination, but these subsections benefit businesses, service providers, and contractors by explaining that they should not turn a blind eye to practices that would essentially require consumers to make repetitive requests to delete with the business, rendering the right to delete pointless. The subsections also benefit consumers in ensuring greater compliance with the law.

Subsection (g)(5) has been added to require a business that denies a request to delete in whole or in part must also inform the consumer that they can file a complaint with the Agency and the Attorney General's office. This is necessary to inform consumers of their ability to complain with the two entities that can enforce the CCPA. This benefits consumers by educating them of their right and helps the Agency and Attorney General enforce the CCPA.

Changes without regulatory effect. Non-substantive changes (e.g., adjustments to punctuation) have been made throughout the section. Subsections have been renumbered.

§ 7023. Requests to Correct.

Subsection (c) has been modified to add language and examples to make clear that businesses, service providers, and contractors are to implement measures to ensure that information subject to a request to correct remains corrected. These modifications are necessary because failure to take these steps could result in continued use and/or dissemination of inaccurate information, which would harm consumers and undermine the right to correct. **Subsections (c)(1) and (2)** are illustrative examples of how to comply with subsection (c), with subsection (c)(2) further clarifying that a business is obligated to correct information stored in a backup or archived system only if that system comes into active use. **Subsection (c)(2)** is intended to minimize the burden on the business of complying with requests to correct and is consistent with regulations pertaining to requests to delete. (*See* Cal. Code Regs., tit. 11, § 7022, subd. (d).) These modifications benefit both businesses and consumers by ensuring that personal information held by the businesses is accurate.

Subsection (f)(3) has been added to require businesses that deny a consumer's request to correct to inform the consumer that, upon the consumer's request, it will note both internally and to any person to whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer. In the Agency's previous rulemaking, it received conflicting public comments regarding whether consumers should be permitted to provide an addendum to businesses about their request, and whether businesses should be required to accept such an addendum even if the request is denied. This subsection aims to balance those conflicting comments by requiring businesses to maintain only a notation, and only at the consumer's request. This requirement is further intended to prevent the proliferation of potentially inaccurate personal information, and acknowledges that in some instances, a consumer may continue to believe contested information is inaccurate even though the business is unable to correct or delete the information or has determined that it is most likely accurate. This benefits consumers by giving them the ability to dispute the accuracy of personal information about them when it is shared. Consistent with subsection (h), a business is not obligated to make or disclose this notation if it determines that the

consumer's request was fraudulent or abusive. This exception aims to minimize the compliance burden on the business, and to protect consumers from potential abuses of the right to correct such as attempted identity theft.

Subsection (f)(4) has been modified to include a requirement that, upon the consumer's request, the business must make the written statement the consumer submits available to any person to whom it discloses, shares, or sells the personal information subject to the request to correct health information. Like the provision in subsection (f)(3), this provision is intended to prevent the proliferation of potentially inaccurate health information. It also gives consumers the ability to dispute the accuracy of personal information about them when it is shared.

Subsection (f)(6) has been added to require businesses that deny a request to correct in whole or in part, it must also inform the consumer that they can file a complaint with the Agency and the Attorney General's office. This is necessary to inform consumers of their ability to complain with the two entities that can enforce the CCPA. This benefits consumers by educating them of their right and helps the Agency and Attorney General enforce the CCPA.

Subsection (i) has been modified to add a requirement that the business provide the name of the source from which it received the alleged inaccurate information, or in the alternative, inform the source that the information provided was incorrect and must be corrected. Naming the source was previously guidance given to businesses, but with this change, the business must either provide the name or inform the source of the incorrect information. The alternative option of telling the source instead of providing the source's name provides flexibility to businesses in responding to consumers while ensuring that a consumer's exercise of their right to correct is meaningfully effectuated. This benefits both consumers and businesses by addressing incorrect information at its source to prevent the further proliferation of inaccurate information about the consumer.

Subsection (j) has been modified to require businesses to provide a way to confirm that certain personal information the business maintains is the same as what the consumer has provided. This was previously guidance given to businesses, but with this change, it is now mandatory. This is necessary to ensure that consumers have the ability to determine whether the personal information the business has about them is correct.

Subsection (k) has been modified to make clear that failing to consider and address the possibility that corrected information may be overridden by inaccurate information subsequently received factors into whether the business, service provider, or contractor has adequately complied with a consumer's request to correct. This is a non-substantive change.

Changes without regulatory effect. Subsections have been renumbered.

§ 7024. Requests to Know.

Subsection (d) has been revised to require businesses to provide a way for consumers to confirm that certain sensitive personal information the business maintains is the same as what the consumer believes it should be. This is necessary to harmonize how businesses are to handle requests to know certain sensitive pieces of personal information with how they are to handle requests to correct regarding those same pieces of personal information. This benefits consumers by giving them a means to know whether the sensitive personal information the business has about them is correct.

Subsection (e) has been reorganized to include the requirement that when a business denies a request to know in whole or in part, it must also inform the consumer that they can file a complaint with the Agency and the Attorney General's office. This is necessary to inform consumers of their ability to complain with the two entities that can enforce the CCPA. This benefits consumers by educating them of their right and helps the Agency and Attorney General enforce the CCPA.

Subsection (k) has been revised to explain a business's disclosure obligations under Civil Code sections 1798.110 and 1798.115 more precisely. **Subsections (k)(3) and (k)(5)** have been revised to include "sharing" as required by Civil Code sections 1798.110, subdivisions (c)(3) and 1798.115, subdivisions (c)(2). **Subsection (k)(4)** has been revised to use "discloses" instead of "shares" to mirror the language in Civil Code section 1798.110, subdivision (c)(4). **Subsection (k)(6)** has been revised to add "service providers or contractors" because disclosures for a business purpose are made to those entities. These changes are necessary to describe the requirements more precisely. They benefit businesses by making clear the business's obligations and also benefit consumers by increasing compliance by businesses.

Subsection (*l*) has been revised to clarify that businesses must identify categories of service providers and contractors in a manner that provides consumers a

meaningful understanding of the categories listed. The addition ensures that the requirement that businesses describe categories meaningfully applies to all categories that businesses are required to disclose.

§ 7025. Opt-Out Preference Signal.

Subsections (c)(3), (4), and (6) have been revised to require businesses to display the consumer's choice as it relates to the sale/sharing of their personal information. Specifically, the business must display whether it has processed the consumer's opt-out preference signal as a valid request to opt-out of sale/sharing on its website. **Subsection (c)(6)** also provides exemplar language for how a business can communicate this information to the consumer.

This regulation is necessary to avoid confusion for consumers about their opt-out state while using a business's website or online services; it will inform consumers whether they are opted out and that the business has processed the opt-out preference signal. It also 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. This regulation also implements Civil Code section 1798.185, subdivision (a)(19)(A)(ii), which states that the opt-out preference signal should be consumer-friendly, clearly described, and easy for the consumer to use. This was previously guidance given to businesses, but with this change, it is now mandatory.

Subsection (f)(3) has been revised to replace "through" with a hyphen. This is a non-substantive change.

§ 7026. Requests to Opt-Out of Sale/Sharing

Subsection (e) has been revised to include the requirement that a business that denies a request to opt-out of sale/sharing must also inform the consumer that they can file a complaint with the Agency and the Attorney General's office. This is necessary to inform consumers of their ability to complain with the two entities that can enforce the CCPA. This benefits consumers by educating them of their right and helps the Agency and Attorney General enforce the CCPA.

Subsection (f)(3) has been added to provide illustrative examples to explain the timing requirements for requests to opt-out of sale/sharing. The first example explains what is meant by "as soon as feasibly possible" within the context of

programmatic advertising technology on a website, and the second example illustrates the requirement in subsection (b)(2). This addition is necessary to provide businesses with further guidance on how to comply with the timing requirements for requests to opt-out of sale/sharing. It benefits businesses by making clear the business's obligations and also benefits consumers by increasing compliance by businesses.

Subsection (g) has been revised to require businesses to provide a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. It also provides exemplar language for how a business can communicate this information to the consumer. This regulation is necessary to avoid confusion for consumers on their opt-out state while using a business's website or online services; it will inform the consumer whether they are opted out and that the business has processed the opt-out preference signal. It also 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. This regulation also implements Civil Code section 1798.185, subdivision (a)(19)(A)(ii), which states that the opt-out preference signal should be consumer-friendly, clearly described, and easy for the consumer to use. This was previously guidance given to businesses, but with this change, it is now mandatory.

§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information.

Subsection (e) has also been revised to replace "should be applied" to "applies" for grammatical reasons. This is a non-substantive change.

Subsection (f) has been revised to include the requirement that when a business denies a request to limit, it must also inform the consumer that they can file a complaint with the Agency and the Attorney General's office. This is necessary to inform consumers of their ability to complain with the two entities that can enforce the CCPA. This benefits consumers by educating them of their right and helps the Agency and Attorney General enforce the CCPA.

Subsection (g)(3) has been revised to replace "shared" with "made available." This change is necessary because "shared" is defined in the statute to apply to cross-context behavioral advertising and this regulation applies to a broader range of

contexts. Using the term "made available" is more precise and benefits businesses by providing clearer guidance on their obligations under the law.

Subsection (h) has been revised to require businesses to provide a means by which the consumer can confirm that their request to limit has been processed by the business. This is necessary to promote transparency and consumer understanding regarding the outcome of their request. The Agency considered the alternative of requiring the business to confirm receipt of the request to limit, but determined that such a requirement was too prescriptive and may create friction in the consumer's user experience. Instead, the Agency determined that requiring a performance-based standard that gives flexibility to the business regarding how to display the status of the consumer's request addresses the need for transparency with a lesser burden to the business to craft the means in accordance with how it manages other CCPA requests. This was previously guidance given to businesses, but with this change, it is now mandatory.

Subsection (m)(2) has been revised to provide an additional example of how sensitive personal information may be used by a business to prevent a security incident that would compromise the confidentiality of stored or transmitted personal information. Scanning the contents of an employee's outgoing emails to prevent the leaking of sensitive personal information outside the business may be a permitted use that is not subject to a consumer's right to limit. However, the example also explains that scanning the emails for other purposes would not fall within this exception to the consumer's right to limit. This example is necessary to demonstrate how the use of sensitive personal information for the purpose of preventing a security incident must be reasonably necessary and proportionate.

Subsection (m)(3) has been revised to provide an additional example of how sensitive personal information may be used to resist malicious, deceptive, fraudulent, or illegal actions directed at the business. A business may use and collect biometric information about their employees to prevent unauthorized access to secured areas of their business and this use would not be subject to a consumer's right to limit. However, the example also explains that the exception does not allow the business to retain this information indefinitely or use it for unrelated purposes, such as the development of commercial products. This is because that use would not be reasonably necessary and proportionate for the purpose of resisting malicious, deceptive, fraudulent, or illegal actions directed at

the business. This example is necessary to clarify for businesses how this exception to the right to limit works.

Changes without regulatory effect. Subsections have been renumbered.

§ 7028. Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information or Limiting the Use and Disclosure of Sensitive Personal Information.

Subsection (a) has been revised to extend the procedures for requests to opt-in to include requests to opt-in to the sharing of personal information and requests to opt-in to the use and disclosure of sensitive personal information. This is necessary to align the regulation with the amended language of the statute, which added a new right to limit the use and disclosure of sensitive personal information. (Civ. Code, § 1798.121.)

Subsection (c) has been added to address situations where consumers initiate transactions with businesses after making a request to limit when those transactions may require that the business disclose or use the consumer's sensitive personal information in a manner inconsistent with the request to limit. In order to balance the consumer's privacy interest with both the consumer's and the business's interest in completing their transaction, this subsection allows a business to obtain the consumer's consent to use or disclose the information for that purpose even if it is within 12 months of the consumer's request during which the business is not allowed to ask for the consumer's consent to reverse their decision. (*See* Civ. Code, § 1798.135, subd. (c)(4).) The subsection further instructs that section 7004 applies to obtaining the consumer's consent. This subsection is necessary to provide guidance to businesses on how to implement the new right to limit and to also ensure that consumers are aware of their rights and can exercise them in an informed manner.

Changes without regulatory effect. The title has been amended to better reflect the content of the regulation.

ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

§ 7050. Service Providers and Contractors.

Subsection (a) has been revised to clarify that the purposes for which a service provider or contractor retains, uses, or discloses personal information must be reasonably necessary and proportionate to serve the purposes listed in the regulation. This change is necessary to remind service providers and contractors that in their retention, use, and disclosure of personal information, they must also apply the data minimization principles set forth in subsection 7002(d). The use for these purposes must be reasonably necessary and proportionate. This change benefits businesses by making clear the business's obligations and also benefits consumers by increasing compliance by businesses.

Subsections (a)(4) has been revised to provide an example of what would be a reasonably necessary and proportionate use of personal information to prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity. This example benefits businesses by providing a clear example of how personal information can be used for this purpose.

Subsection (a)(5) has been revised to delete "through (a)(7)". This is a non-substantive change required by revisions to the statute.

Subsection (h) has been added to require that service providers and contractors cooperate with businesses for those businesses' cybersecurity audits and risk assessments. **Subsection (h)** specifies that this requirement is only with respect to the personal information that the service provider or contractor has collected pursuant to their written contract with the business. **Subsection (h)(1)** explains that cooperating with a business's completion of its cybersecurity audit includes making available to the business's auditor all relevant information that the auditor requests as necessary to complete the audit and not misrepresenting any fact that the auditor deems relevant to the audit. **Subsection (h)(2)** explains that cooperating with a business that is conducting a risk assessment includes making available to the business all facts necessary to conduct the risk assessment and not misrepresenting any fact necessary to conduct the risk assessment.

Because businesses may be using service providers or contractors when processing personal information in ways that present significant risk to consumers' privacy or security, this regulation is necessary to ensure that they have visibility into what

their service providers or contractors are doing as part of that processing. Otherwise, a business's auditor would lack sufficient information to complete the business's cybersecurity audit (e.g., the auditor would lack information to conduct an audit if a business is using a service provider to implement parts of its cybersecurity program). Similarly, the business would lack sufficient information to conduct their risk assessments (e.g., the business may not have sufficient information to identify operational elements of the activity or corresponding risks to consumers' privacy). In addition, this regulation clarifies that cooperation involves making necessary information available to the business and not misrepresenting relevant or necessary facts, which is necessary to ensure that businesses have full and accurate information when they are completing cybersecurity audits or conducting risk assessments.

§ 7051. Contract Requirements for Service Providers and Contractors.

Subsection (a)(4) has been deleted because it is duplicative of subsection (a)(3).

Subsection (a)(5) has been revised to include additional examples of requirements that a business may include in its contracts with service providers or contractors, such as requiring the service provider or contractor to assist the business in completing the business's cybersecurity audit, conduct risk assessments, or comply with the business's ADMT requirements.

This revision is necessary to provide clarity and guidance to businesses about how to operationalize the CCPA's requirement that contracts with service providers and contractors must require these entities to comply with all applicable sections of the CCPA and these regulations (e.g., subsection 7050(h)) and to provide the same level of privacy protections as required of businesses by the CCPA and these regulations. These examples also ensure alignment between the contractual requirements for service providers and contractors set forth in this subsection, and the requirements for service providers and contractors set forth in subsection 7050(h) (specifically, that the service provider and contractor must cooperate with the business for cybersecurity audits and risk assessments). By incorporating the requirements of service providers and contractors directly into contracts, the business can further ensure that the service provider and contractor are fully aware of their responsibilities when cooperating with the business to comply with the CCPA's requirements.

Subsection (c) has also been revised to delete "depending on the circumstances" because they are unnecessary. This is a non-substantive change.

Changes without regulatory effect. The subsections have been renumbered.

§ 7053. Contract Requirements for Third Parties.

Subsection (b) has been modified to delete "depending on the circumstances" to delete superfluous words. This is a non-substantive change.

ARTICLE 5. VERIFICATION OF REQUESTS

§ 7060. General Rules Regarding Verification.

Subsection (a) has been revised to include "request to access ADMT." This revision is necessary because subsection 7222(d) requires that businesses verify the identity of the person making the request to access ADMT as set forth in Article 5. This revision is necessary to ensure consistency throughout the regulations and clarify that the verification requirements in Article 5 apply to requests to access ADMT. This verification requirement balances the consumer's right to access ADMT with their interest in preventing the disclosure of their personal information to unauthorized persons. It also benefits businesses by enabling them to leverage existing verification processes for other CCPA rights and extend them to the right to access ADMT.

Subsection (b) has been revised to include "to make a request to opt-out of ADMT." This regulation is necessary to ensure that consumers can exercise their right to opt-out of ADMT without unnecessary impediments. It also addresses observations in the marketplace and comments received during prior preliminary rulemaking activities that some businesses have misused the verifiable request process to impede consumers' exercise of their other opt-out rights. This subsection also recognizes that, in some cases, a business may need additional information from a consumer to process a request to opt-out of ADMT and permits businesses to request additional information but only insofar as it is needed. Lastly, this revision also ensures consistency with how the other opt-out rights (i.e., requests to opt-out of sale/sharing and requests to limit) address verification.

Subsections (c)(1) and (d) have been revised to delete unnecessary words and to strengthen language requiring businesses to first consider how they can verify a

consumer's identity using personal information that it already maintains about the consumer before asking the consumer to provide additional information.

Subsection (e) has been revised to change "may" to "must" and to add that a business that compensates the consumer for the cost of the notarization must provide the consumer with instructions on how they will be reimbursed prior to the consumer's submission of the notarization. This change has been made in response to comments received by the Agency and is necessary to address business practices that undermine a consumer's ability to use an authorized agent to submit a CCPA request.

Subsection (f) has been revised to add "access to information about a business's use of automated decisionmaking technology with respect to a consumer." This revision is necessary to protect consumers' personal information during submission and transmission of information for requests to access ADMT.

Subsection (h) has also been revised to delete the word "make an effort to" to make clear that the business must not use personal information that is the subject of a request to correct to verify the consumer.

These changes benefit businesses by further clarifying businesses' obligations regarding authorized agents. Consumers will also benefit from the increased compliance by businesses.

§ 7062. Verification for Non-Accountholders.

Subsection (c) has been revised to add "requests to access ADMT." This revision is necessary to ensure that businesses satisfy a standard of a reasonably high degree of certainty when processing requests to access ADMT, if they do not have an account with the consumer. Due to the sensitivity of some information subject to a request to access ADMT (e.g., details regarding hiring decisions or public profiling), it is important that consumers are verified with a reasonably high degree of certainty before the business provides them with information in response to a request to access ADMT. This addition also benefits businesses because it enables them to leverage existing verification processes for requests to know and extend them to requests to access ADMT.

Subsection (e)(2) has been revised to fix a typographical error in its reference to section 7060. This is a non-substantive change.

Subsection (f) has been revised to add "request to access ADMT." This revision is necessary to operationalize the requirements for requests to access ADMT. Specifically, it is necessary to clarify what the business must do if it cannot verify the identity of the requestor for a request to access ADMT (i.e., the business must deny the request).

§ 7063. Authorized Agents.

Subsection (a) has been revised to clarify that businesses shall not require consumers to resubmit their request in their individual capacity. This change has been made in response to comments received by the Agency and is necessary to make clear that such a business practice would undermine a consumer's ability to use an authorized agent to submit a CCPA request. This revision benefits businesses by making clear the business's obligations regarding authorized agents. Consumers will also benefit from the increased compliance by businesses.

ARTICLE 6. SPECIAL RULES REGARDING CONSUMERS LESS THAN 16 YEARS OF AGE

Change without regulatory effect. The title of the article has been revised to use the term "less than" instead of "under" to be consistent with the content within the article.

§ 7070. Consumers Under 13 Years of Age.

Changes without regulatory effect. Non-substantive changes (e.g., adding spaces to subsections (a) to (f)) have been made within the section.

ARTICLE 7. NON-DISCRIMINATION

§ 7080. Discriminatory Practices.

Subsection (c) has been revised to include "request to access ADMT" and "request to opt-out of ADMT." This revision is necessary to align this regulation with consumers' rights to access and opt-out of ADMT. Specifically, it is necessary to clarify the non-discriminatory bases on which a business may deny a request to access or opt-out of ADMT, to avoid confusion for businesses when they are relying on an exception to the ADMT requirements set forth in Article 11.

ARTICLE 8. TRAINING AND RECORD-KEEPING

§ 7102. Requirements for Businesses Collecting Large Amounts of Personal Information.

Subsection (a)(1)(D) has been added to require the compilation and disclosure of metrics for requests to access ADMT that the business received, complied with in whole or in part, and denied. **Subsection (a)(1)(G)** has been added to similarly require this for requests to opt-out of ADMT. This is necessary to inform the Agency, Attorney General, policymakers, academics, and members of the public about businesses' compliance with the CCPA. It considers the burden on businesses to compile and post this information by limiting the requirement to those businesses that handle a large amount of personal information, specifically, the personal information of approximately 10 percent of California's total population or more. Based on its experience and available information, the Agency determined that 10 percent or more of California's total population was an appropriate threshold.

Changes without regulatory effect. The subsections have been renumbered.

ARTICLE 9. CYBERSECURITY AUDITS

Civil Code section 1798.185, subdivision (a)(15)(A), requires the Agency to issue regulations that do three main things: (1) require businesses to perform a cybersecurity audit on an annual basis when their processing of consumers' personal information presents significant risk to consumers' security; (2) define the scope of the cybersecurity audit; and (3) establish a process to ensure that the audits are thorough and independent. The statute also directs 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. The purpose of Article 9 is to operationalize the concepts introduced by the CPRA, and to provide clarity and specificity to implement the law. The provisions are necessary to fulfill the Agency's obligations under Civil Code section 1798.185, subdivision (a)(15)(A), and to provide clarity and guidance for businesses about how to perform an annual cybersecurity audit. This section is informed by public comments received by the Agency during preliminary rulemaking activities, cybersecurity and auditing approaches in other frameworks, and the purpose and intent set forth in

the CPRA. This section also benefits businesses and consumers, because cybersecurity audits help businesses to identify and address cybersecurity vulnerabilities, motivate businesses' senior leadership to invest in improving the business's cybersecurity, and mitigate the negative impacts of unauthorized access, destruction, use, modification, or disclosure of personal information; and unauthorized activity resulting in the loss of availability of personal information.[14]

§ 7120. Requirement to Complete a Cybersecurity Audit.

Subsections (a) and (b) collectively restate and operationalize the statutory direction that businesses whose processing of consumers' personal information presents significant risk to consumers' security perform a cybersecurity audit. Subsection (a) restates the statutory language and cross-references subsection (b), which explains which businesses' processing presents significant risk to consumers' security. Subsections (a) and (b) are necessary to clarify for businesses when their processing presents "significant risk to consumers' security" and, therefore, when they must complete a cybersecurity audit. Section 7120 benefits businesses, their auditors, and consumers by providing clarity and guidance regarding which businesses must perform cybersecurity audits.

Subsection (b)(1) states that a business that "meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(C), in the preceding calendar year" (i.e., "derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information" in the preceding calendar year) is a business whose processing of consumers' personal information presents significant risk to consumers' security. As set forth above, Civil Code section 1798.185, subdivision

---

[14] *See, e.g.,* NAT'L INST. OF STANDARDS & TECH., NIST CYBERSECURITY FRAMEWORK (CSF) VERSION 2.0 13 (Feb. 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf; *Cybersecurity Program Audit Guide*, GAO-23-104705, U.S. GOV'T ACCOUNTABILITY OFFICE (2023), https://www.gao.gov/assets/d23104705.pdf; INFORMATION SECURITY PROGRAM AUDIT, CAL. DEP'T OF TECH., https://cdt.ca.gov/security/information-security-program-audit-services/; *California Consumer Privacy Act Regulations, Pre-Rulemaking Informational Sessions*, Transcript at 56–66, 57, 63, 67, CAL. PRIV. PROT. AGENCY (Mar. 30, 2022), *available at* https://cppa.ca.gov/meetings/materials/20220330_transcript.pdf; Sergeja Slapničar et al., *Effectiveness of Cybersecurity Audit*, 44 INT'L J. OF ACCT. INFO. SYS., 10054 (2022), https://doi.org/10.1016/j.accinf.2021.100548; Paul John Steinbart et al., *The Relationship Between Internal Audit and Information Security: An Exploratory Investigation*, 13 INT'L J. OF ACCT. INFO. SYS. 3, 228–243 (Sept. 2012), https://doi.org/10.1016/j.accinf.2012.06.007; He Li et al., *The Impact of Audit Office Cybersecurity Experience on Nonbreach Client's Audit Fees and Cybersecurity Risks*, 1 INT'L J. OF ACCT. INFO. SYS. 38 (1): 177–206 (Mar. 2024), https://doi.org/10.2308/ISYS-2023-014.

(a)(15)(A), directs the Agency to consider the 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. Deriving 50 percent or more of one's annual revenues from selling or sharing consumers' personal information pertains to the nature of a business's processing activities, and it can be a proxy for the complexity of the business and the scope of its processing activities. For example, such businesses may "collect and trade vast amounts of personal information, to track [consumers] across the internet, and to create detailed profiles of their individual interests." (*See* Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 2(I).) Processing and selling or sharing vast amounts of personal information presents significant risk to consumers' security. In addition to the privacy risks identified in the discussion of subsection 7150(b)(1) regarding businesses' sale/sharing of consumers' personal information, the more personal information a business collects, the more risk it presents to consumers' security. For example, there will be more personal information at risk if a bad actor manages to exploit gaps or weaknesses in a business's cybersecurity program. Similarly, the more third parties to whom a business sells or shares consumers' personal information, the more risk it presents to consumers' security. For example, there will be more information systems that a bad actor could compromise to obtain unauthorized access to consumers' personal information. When consumers' personal information is subject to unauthorized access, consumers suffer harms, as set forth in subsection 7152(a)(5) of the regulations, and as discussed in more detail in the discussion of subsection 7152(a)(5). This provision is necessary to clarify that such businesses' processing of consumers' personal information presents "significant risk to consumers' security," and that they must therefore complete an annual cybersecurity audit.

Subsection (b)(2) states that a business that meets an annual gross revenue threshold and one of two processing thresholds in the preceding calendar year presents significant risk to consumers' security. The specified annual gross revenue threshold is set forth in Civil Code section 1798.140, subdivision (d)(1)(A). This threshold is currently $27,975,000.00. (*See* subsection 7005(b)(1).) The two processing thresholds are the business processed (1) the personal information of 250,000 or more consumers or households, or (2) the sensitive personal information of 50,000 or more consumers. Civil Code section 1798.185, subdivision (a)(15)(A), 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.

Meeting the annual gross revenue threshold, in combination with meeting the personal-information-processing thresholds pertains to size and complexity of the business, and the nature and scope of its processing activities. Revenue is a proxy for a business's size[15] and may logically be a proxy for the complexity of a business. The personal-information processing thresholds pertain to the nature and scope of the business's processing activities. In addition to the privacy risks identified in the discussion of subsection 7150(b)(2) regarding businesses' processing of consumers' sensitive personal information, the more personal information (including sensitive personal information) a business processes, the more risk it presents to consumers' security. For example, there will be more personal information (including sensitive personal information) at risk if a bad actor manages to exploit gaps or vulnerabilities in the business's cybersecurity program).[16] When consumers' personal information is subject to, for example, unauthorized access, consumers suffer harms, as set forth in subsection 7152(a)(5) of the regulations, and as addressed in more detail in the discussion of subsection 7152(a)(5). Subsection (b)(2) is necessary to clarify that such businesses' processing of consumers' personal information presents "significant risk to consumers' security," and that they must therefore complete an annual cybersecurity audit.

Leveraging the annual gross revenue threshold from the statute benefits businesses because it is something they likely already consider in determining whether they are a "business" subject to the CCPA. The section includes 250,000 and 50,000 as the personal-information-processing thresholds because these represent significant numbers of consumers whose security is at risk due to the business's processing their personal information.

---

[15] *See, e.g.*, *Size Standards*, U.S. Small Bus. Admin., https://www.sba.gov/federal-contracting/contracting-guide/size-standards.

[16] *See, e.g.*, Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMM'N.: BUS. BLOG (Aug. 31, 2016) https://www.ftc.gov/business-guidance/blog/2016/08/nist-cybersecurity-framework-and-ftc.

§ 7121. Timing Requirements for Cybersecurity Audits.

The purpose of section 7121 is to provide clarity and guidance to businesses regarding when they must comply with their statutory obligation to complete annual cybersecurity audits. It is necessary to implement and operationalize the business's requirements to complete an annual cybersecurity audit. It also benefits businesses and consumers by providing clarity and guidance regarding when businesses must complete annual cybersecurity audits.

Subsection (a) states that a business has 24 months from the effective date of these regulations to complete its first cybersecurity audit. It balances the need to ensure that businesses complete thorough and independent cybersecurity audits while giving those businesses sufficient time to establish the processes to ensure that their first and subsequent cybersecurity audits will be thorough and independent. It is necessary to clarify for businesses when they must complete their first cybersecurity audit.

Subsection (b) states that the business's subsequent cybersecurity audits must be completed every calendar year, and that there must be no gap in the months covered by successive cybersecurity audits. It is necessary to clarify for businesses when they must complete their subsequent cybersecurity audits and to ensure that their cybersecurity audits are thorough.

Subsections (a) and (b) together provide flexibility for businesses as to when during the initial 24-month period following the effective date of Article 9 of these regulations they may complete their initial cybersecurity audit, and, therefore, when they must complete their subsequent audits, while clarifying that there cannot be gaps in the months covered by successive audits. This approach reduces the burden on businesses, while ensuring that cybersecurity audits cover all months, so that there will be no gap in audits of how businesses protect consumers' personal information.

§ 7122. Thoroughness and Independence of Cybersecurity Audits.

The purpose of section 7122 is to establish processes for businesses and their auditors to follow to ensure the thoroughness and independence of the business's annual cybersecurity audits. The section is necessary because Civil Code section 1798.185, subdivision (a)(15)(A), requires the Agency to establish a process to ensure that audits are thorough and independent. It also benefits businesses, their

auditors, and consumers by providing clarity and guidance regarding how businesses must complete a thorough and independent cybersecurity audit. Processes supporting auditor independence also help to ensure that cybersecurity vulnerabilities are properly identified, assessed, and documented,[17] benefiting businesses and consumers.

Subsection (a) provides clarity and guidance for businesses regarding how they can ensure that their audits are independent. Subsection (a) specifies that a business must conduct its audit using a qualified, objective, independent professional ("auditor") who uses procedures and standards generally accepted in the profession of auditing. This subsection is necessary because Civil Code section 1798.185, subdivision (a)(15)(A), requires the Agency to establish a process to ensure that audits are thorough and independent, and this subsection clarifies how businesses must ensure auditor independence. Requiring that auditors be qualified, objective, and independent is consistent with approaches taken in the current

[17] Academic scholarship notes the risks to auditors' independence. *See, e.g.,* Sarah Beckett Ference, *Auditor Independence Threats and Malpractice Claims*, J. OF ACCT. (Dec. 1, 2023), https://www.journalofaccountancy.com/issues/2023/dec/auditor-independence-threats-and-malpractice-claims.html; Chris Jay Hoofnagle, *Assessing the Federal Trade Commission's Privacy Assessments*, 14(2) IEEE SECURITY & PRIVACY 58–64 (Mar./Apr. 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2707163; Abigail Brown, *Institutional Corruption of the Audit Profession*, Edmond & Lily Safra Ctr. for Ethics (2010-2011 Seminars), https://ethics.harvard.edu/abigail-brown-institutional-corruption-audit-profession; Abigail Brown, *The Economics of Auditor Capture: Implications for Empirical Research*, 1-2, 18-21, Edmond & Lily Safra Ctr. for Ethics (2012), https://abigailbrown.wordpress.com/wp-content/uploads/2009/08/auditor-capture.pdf.

The importance of auditors' independence is commonly acknowledged. *See, e.g., AS 1005.01–02: Auditing Standards*, PCAOB (2020), https://assets.pcaobus.org/pcaob-dev/docs/default-source/standards/auditing/documents/auditing_standards_audits_after_december_15_2020.pdf?sfvrsn=5862544e_4; CODIFICATION OF ACCT. STANDARDS & PROCS., Statement on Auditing Standards No. 113, § 150.02 (AM. INST. OF CERTIFIED PUB. ACCTS. 2006), https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/au-00150.pdf; *Code of Professional Ethics*, ISACA, https://www.isaca.org/code-of-professional-ethics; Auditor Independence Matters, U.S. SECS. & EXCH. COMM'N, https://www.sec.gov/page/oca-auditor-independence-matters; Final Rule: Improper Influence on Conduct of Audits, Exchange Act Release No. 34-47890 (May 20, 2003), 17 C.F.R. pt. 240, https://www.govinfo.gov/content/pkg/FR-2003-05-28/pdf/03-13095.pdf.

marketplace in other contexts, such as FTC orders and auditing organizations' auditing standards.[18]

Subsections (a)(1) and **(a)(2)** provide further clarity and guidance as to what auditor objectivity and independence mean, and how businesses must preserve auditor independence, drawing from practices in the current marketplace in other contexts.[19] For example, **subsection (a)(1)** clarifies that the auditor may be internal or external to the business but must exercise impartial judgment, be free to make decisions and assessments without influence by the business, and not participate in the very business activities that the auditor may assess in the current or subsequent cybersecurity audits. **Subsection (a)(2)** clarifies that if a business uses an internal auditor, the auditor must report directly to, and have their performance-evaluation and compensation determined by, the business's board, governing body, or — if neither of those exists — to the business's highest-ranking executive who does not have direct responsibility for the cybersecurity program. The measures of organizational independence from those with direct responsibility for the business's cybersecurity program make it more likely that the auditor can maintain the independence and objectivity articulated in subsection (a)(1). These subsections

---

[18] *See, e.g.*, Final Decision and Order at 8, Blackbaud, Inc., FTC Docket No. C-4804 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2023181_blackbaud_final_consent_package.pdf; Final Decision and Permanent Injunction at 33-34, People v. Equifax, Inc., No. CGC-19-577800 (Super. Ct. S.F. City and County, 2019), https://oag.ca.gov/system/files/attachments/press-docs/Equifax%20-%20Final%20approved%20%20judgment.pdf; FTC v. Equifax, Inc., No.1:19-cv-03297-TWT (N.D. Ga. July 23, 2019), Stipulated Order for Permanent Injunction and Monetary Judgment at 19, (N.D. Ga., Jul. 23, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_order_signed_7-23-19.pdf; *AS 1001.04, 1010.01, 1015.07–08, Auditing Standards*, PCAOB (2020), https://assets.pcaobus.org/pcaob-dev/docs/default-source/standards/auditing/documents/auditing_standards_audits_after_december_15_2020.pdf?sfvrsn=5862544e_4; CODIFICATION OF ACCT. STANDARDS & PROCS., Statement on Auditing Standards No. 113, §§ 150.01, 150.02 (AM. INST. OF CERTIFIED PUB. ACCTS. 2006); *Code of Professional Ethics*, ISACA, https://www.isaca.org/code-of-professional-ethics; INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, IT AUDIT FRAMEWORK (ITAF): A PROFESSIONAL PRACTICES FRAMEWORK FOR IT AUDIT, (4th Ed. 12, 2020), www.isaca.org/itaf.

[19] *See, e.g.*, FED. FIN. INST. EXAMINATION COUNCIL, *FFIEC IT Examination Handbook*, https://ithandbook.ffiec.gov/it-booklets/audit/independence-and-staffing-of-internal-it-audit/independence/; GOV. CODE § 13887; INS. CODE § 900.3(c), (d)(1); N.Y. COMP. CODES R. & REGS. tit. 23, § 500.1(h); Final Judgment and Permanent Injunction, People v. Upward Labs Holdings, Inc., et al., CGC-20-586611 (Super. Ct. S.F. City and County, 2020), https://oag.ca.gov/sites/default/files/People%20v.%20Glow%20-%20Final%20Judgment%20and%20Permanent%20Injunction%20-%2007374856.pdf; ISACA, INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, IT AUDIT FRAMEWORK (ITAF): A PROFESSIONAL PRACTICES FRAMEWORK FOR IT AUDIT, (4th Ed. 12, 2020), www.isaca.org/itaf.

together provide necessary clarity for businesses as to how they must ensure auditor independence.

Subsections (b)–(e) provide clarity and guidance for businesses and their auditors regarding how to ensure the business's audit is thorough and independent.

Specifically, **subsection (b)** specifies that the business must make all information available to the auditor that the auditor requests as relevant to the cybersecurity audit. This subsection is necessary because an audit cannot be thorough and independent unless the auditor has the information they deem necessary to make determinations about the scope of the audit (e.g., which systems the audit will evaluate) and the criteria it will evaluate (e.g., how the audit will assess the systems). Subsection (b) is informed by information and public comments received by the Agency during preliminary rulemaking activities about the risks of businesses defining the contours of their own audits, and by frameworks in other contexts.[20]

Subsection (c) specifies that the business must make good-faith efforts to disclose to the auditor all facts relevant to the cybersecurity audit and must not misrepresent in any manner any fact relevant to the cybersecurity audit. This subsection is necessary because an audit cannot be thorough and independent unless the auditor has full and accurate information to make their independent decisions and assessments throughout the course of the audit. It is also consistent with the federal government's approach to ensuring that auditors are provided with full and accurate information in other contexts, such as settlements that include

[20] *See, e.g., California Consumer Privacy Act Regulations, Pre-Rulemaking Informational Sessions*, Transcript at 56–66, 59, CAL. PRIV. PROT. AGENCY (Mar. 30, 2022), *available at* https://cppa.ca.gov/meetings/materials/20220330_transcript.pdf; Final Decision and Order at 9–10, Blackbaud, Inc., FTC Docket No. C-4804 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2023181_blackbaud_final_consent_package.pdf; *AS 1001.05, Auditing Standards*, PCAOB (2020), https://assets.pcaobus.org/pcaob-dev/docs/default-source/standards/auditing/documents/auditing_standards_audits_after_december_15_2020.pdf?sfvrsn=5862544e_4; *Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation* 9, PCI SECURITY STANDARDS COUNCIL (Dec. 2016), https://listings.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf.

independent assessments, and in the context of public companies providing information to their accountants in connection with an audit.[21]

Subsection (d) specifies that the audit must articulate its scope and criteria; identify the specific evidence examined to make decisions and assessments; and explain why the scope, criteria, and evidence are appropriate and why the specific evidence examined is sufficient to justify the auditor's findings. It is designed to provide necessary flexibility to auditors, recognizing that their approaches will vary in scoping an audit, determining the criteria they will use, and determining the evidence they will examine. It is necessary because requiring the auditor to explain these key components helps to ensure the audit's thoroughness, requires the auditor to be thoughtful about what they evaluated, how they evaluated it, what they concluded, and why; and requires them to explain all of that in a way that would enable another person to understand it.

Subsection (d) further specifies that no finding may rely primarily on assertions or attestations by the business's management and must instead rely primarily upon specific evidence that the auditor examined. This is necessary to ensure the thoroughness and independence of audits, including to ensure that audit findings rely upon independent evidence such as documentation, tests, and interviews with relevant employees. These concepts are supported by, and are consistent with, public comments received by the Agency during preliminary rulemaking activities, academic scholarship, and approaches to ensuring auditors' independence in other contexts, such as FTC orders and auditing standards.[22]

Together with the requirements in subsections (h) and (i) that ensure that the most senior individuals in the business review and understand the cybersecurity audit

---

[21] *See, e.g.,* Final Decision and Order at 9–10, Blackbaud, Inc., FTC Docket No. C-4804 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2023181_blackbaud_final_consent_package.pdf; 17 C.F.R. § 240.13b2-2.

[22] *See, e.g.,* Chris Jay Hoofnagle, *Assessing the Federal Trade Commission's Privacy Assessments*, 14(2) IEEE SECURITY & PRIVACY 58–64 (Mar./Apr. 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2707163; Don A. Moore et al., *Conflicts of Interest and the Case of Auditor Independence: Moral Seduction and Strategic Issue Cycling*, 31 ACAD. OF MGMT REV. 10-29, 17 (2006), https://faculty.wharton.upenn.edu/wp-content/uploads/2012/04/Tetlock_2006-auditorsmooreetalpiece.pdf; Final Decision and Order at 9, Blackbaud, Inc., FTC Docket No. C-4804 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2023181_blackbaud_final_consent_package.pdf; *AS 1015.07–1015.09, Auditing Standards*, PCAOB (2020), https://assets.pcaobus.org/pcaob-dev/docs/default-source/standards/auditing/documents/auditing_standards_audits_after_december_15_2020.pdf?sfvrsn=5862544e_4.

findings; and the requirements in subsection 7121(b) that require the business to complete cybersecurity audits every calendar year, the requirements in subsection (d) create opportunities for businesses and their auditors to continually improve both the businesses' cybersecurity posture and the auditing process.

Subsection (e) specifies that the audit must assess, document, and summarize each applicable component of the business's cybersecurity program that is set forth in section 7123, and specifically identify gaps or weaknesses in the business's cybersecurity program. It also requires that the audit specifically address the status of any gaps or weaknesses identified in any prior cybersecurity audit, and any corrections or amendments to any prior cybersecurity audit. These details are necessary to clarify what must be done to ensure that the current audit is thorough, and they also enable businesses to address vulnerabilities in how they protect consumers' personal information. Documenting this information also benefits businesses and their auditors by ensuring the consistency of successive audits' coverage. It also helps successive auditors to understand the business's cybersecurity posture over time, especially when the business engages different auditors from one year to the next and when there is turnover within the business of those responsible for the business's cybersecurity program or for the business's cybersecurity audit compliance.

Subsection (f) requires the audit to include the auditor's name, affiliation, and relevant qualifications. The purpose of the regulation is to document who conducted the audit and their qualifications in case questions arise about the audit or auditor. Additionally, this information will allow future auditors to contact prior auditors if needed, which helps to ensure the thoroughness of successive audits. This regulation is necessary because without this information, the business and its successive auditors would not have consistent insights into successive auditors' qualifications nor a starting point from which to reach out to prior auditors. It also provides accountability and an assurance of the audit's independence and, together with subsection (j), will assist in enforcement.

Subsection (g) requires the audit to include a statement signed and dated by each auditor certifying that they completed an independent review of the business's cybersecurity program and information system, exercised objective and impartial judgment, and did not rely primarily on assertions or attestations by the business's management. The purpose of this subsection is to confirm that the requirements for the audit have been met; it works in tandem with the substantive requirements of

auditor independence in subsections (a) and (d). It is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and independent by requiring that the auditor certify the independence of their audit. It benefits businesses and their auditors by providing assurance that the audit has met the independence requirements.

Subsection (h) requires the audit to be reported to the business's board, governing body, or—if neither of those exists—the business's highest-ranking executive responsible for its cybersecurity program. The purpose of this subsection is to ensure that such individuals are informed about the business's cybersecurity posture, which furthers the intent and purpose of the CCPA to protect consumers' personal information, because reporting to these individuals can help to ensure that the audit itself is thorough. Knowing that the audit will be reported to these individuals will likely motivate businesses to dedicate the appropriate resources and ensure that the audit will be of the highest quality.[23] This subsection is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and independent by requiring that the most senior individuals in the business responsible for its cybersecurity program review and understand the audit results. This subsection is also necessary to enable these individuals to certify the independence of the audit in subsection (i).

Subsection (i) requires the audit to include a statement that is signed and dated by a member of the business's board, governing body, or—if neither of those exists—the business's highest-ranking executive with authority to certify on behalf of the business and who is responsible for its cybersecurity program. The statement must include the signer's name and title and contain language certifying that the business did not influence, and made no attempt to influence, the auditor's decisions or assessments. The signer must also certify in that statement that they have reviewed, and understand the findings of, the cybersecurity audit. The purpose of this subsection is to preserve the independence of the auditor's decisions and assessments and to ensure that the most senior individuals in the business are informed about the business's cybersecurity posture through the audit results. It is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and independent, and to address the risks that businesses

[23] *See infra* note 25.

will seek to influence auditors' assessments of their cybersecurity posture.[24] This subsection provides a reminder as well as an assurance of, and accountability for, the independence of the business's audit. It is also necessary to ensure that the most senior individuals in the business are aware of the audit results—in particular the gaps and weaknesses in the business's cybersecurity program. This enables the business further protect consumers' personal information. Reporting to the board and requiring board accountability for cybersecurity results in more attention and resources being dedicated to cybersecurity and the protection of consumers' personal information.[25] This subsection is also consistent with cybersecurity and auditing approaches in other contexts and frameworks such as the FTC's Standards for Safeguarding Customer Information, the NIST Cybersecurity Framework, the California Government Code, and the NYDFS Cybersecurity Regulations.[26]

Subsection (j) requires the auditor to retain all documents relevant to each cybersecurity audit for a minimum of five (5) years after completion of the cybersecurity audit. This subsection is necessary to specify the duration that auditors must retain documents relevant to cybersecurity audits, which would enable the business to demonstrate compliance with the CCPA and these regulations. The Agency has five years to bring an administrative action alleging a violation of the CCPA; thus, requiring records be maintained for this period of time

---

[24] *See supra* note 17.

[25] *See supra* note 14. *See also* Jared Ho, *Corporate Boards: Don't Underestimate Your Role in Data Security Oversight*, FED. TRADE COMM'N (Apr. 28, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/corporate-boards-dont-underestimate-your-role-data-security-oversight; Megan Gale et al., *Governing Cybersecurity from the Boardroom: Challenges, Drivers, and Ways Ahead*, 121 COMPUTERS & SECURITY 102840, 24 (2022); Slapničar et al., *Effectiveness of Cybersecurity Audit*, 44 INT'L J. OF ACCT. INFO. SYS., 100548 (2022) at 5, https://doi.org/10.1016/j.accinf.2021.100548; Paul John Steinbart et al., *The Influence of a Good Relationship Between the Internal Audit and Information Security Functions on Information Security Outcomes*, 71 ACCT. ORG. & SOC'Y., 15, 15–29 (2018), https://doi.org/10.1016/j.aos.2018.04.005; Sharif Islam et al., *Factors Associated With Security/Cybersecurity Audit by Internal Audit Function, An International Study*, 33 MANAGERIAL AUDITING JOURNAL 4, 377-409 (2018), www.emeraldinsight.com/0268-6902.htm.

[26] *See, e.g.,* 16 C.F.R. § 314.4(i)**;** NAT'L INST. OF STANDARDS & TECH., NIST CYBERSECURITY FRAMEWORK (CSF) VERSION 2.0 10 (Feb. 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf; Gov. Code §§ 13885(b), 13887; N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.3, 500.4; Final Decision and Order at 4, 10, Blackbaud, Inc., FTC Docket No. C-4804 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2023181_blackbaud_final_consent_package.pdf; 17 C.F.R. § 229.106(c)(1); ISACA, INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, IT AUDIT FRAMEWORK (ITAF): A PROFESSIONAL PRACTICES FRAMEWORK FOR IT AUDIT, (4th Ed. 12, 2020), www.isaca.org/itaf.

assists with enforcement.[27] It also benefits businesses by giving them clear direction on how to comply with the law and these regulations. This subsection is also necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough, by enabling the business and its successive auditors to obtain information from prior audits. Such information is necessary to comply with subsections (e)(3) and (4), which require the current audit to address the status of gaps or weaknesses identified in any prior audit, and to identify corrections or amendments to any prior audit.

§ 7123. Scope of Cybersecurity Audit.

The purpose of section 7123 is to ensure the thoroughness of the business's annual cybersecurity audit and define the scope of it. This section articulates the components of a business's cybersecurity program, which an audit must identify, assess, and document. This section benefits businesses and their auditors by providing clear guidance about how to complete a thorough cybersecurity audit. The section is necessary because Civil Code section 1798.185, subdivision (a)(15)(A), requires the Agency to establish a process to ensure that audits are thorough and to define the scope of the audit.

Subsections (a) and (b) provide guidance and clarity for businesses, their auditors, and consumers about what the cybersecurity audit must cover, substantively. Together, they balance the need for the regulations to be both specific and flexible; they recognize the varying ways in which a business may protect consumers' personal information, and the common components of businesses' cybersecurity programs.

Specifically, **subsection (a)** requires the audit to assess and document how the business's cybersecurity program protects personal information from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information.

Proposed subsection (b)(1) requires the audit to identify, assess, and document the business's cybersecurity program, including the related written documentation of the program such as its policies and procedures, and the components listed in subsection (b)(2). It also describes the business's cybersecurity program as

---

[27] *See* CIV. CODE, § 1798.199.70.

"appropriate to the business's size and complexity and the nature and scope of its processing activities, taking into account the state of the art and cost of implementing the components of a cybersecurity program," which is consistent with cybersecurity requirements and guidance in other contexts, such as the FTC's Standards for Safeguarding Customer Information, the European Union's GDPR, and settlements reached between companies and the Attorney General.[28] "Cybersecurity program" is defined in subsection 7001(m).

Thus, subsections (a) and (b)(1) together effectively require the audit to thoroughly assess and document how the business protects consumers' personal information. These requirements are necessary for the cybersecurity audit to identify gaps and weaknesses in its cybersecurity program, which the business can then prioritize and remediate. These subsections recognize that businesses may protect consumers' personal information in varying ways; they provide flexibility for businesses and their auditors to respectively explain, assess, and document how the business protects consumers' personal information.

Subsection (b)(2) requires the audit to identify, assess, and document each of 18 components of the business's cybersecurity program, as applicable; and if not applicable, to document why the component is not necessary to protect consumers' personal information and how the safeguards the business has in place provide at least equivalent security.

Specifically, subsection (b)(2) includes (1) authentication, including multi-factor authentication and strong unique passwords or passphrases; (2) encryption of personal information, at rest and in transit; (3) zero trust architecture; (4) account management and access controls, including restricting each person's privileges and access to personal information to what is necessary for that person to perform their duties; restricting the number of privileged accounts, restricting their access-functions to only those necessary to perform the account-holder's job, and restricting their use to only when necessary to perform functions, and using a

---

[28] *See, e.g.,* 16 C.F.R. § 314.3; Regulation 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 25, 32, 2016 O.J. (L 119) (EU) [hereinafter GDPR]; Final Judgment and Permanent Injunction, People v. Upward Labs Holdings, Inc., et al., CGC-20-586611 (Super. Ct. S.F. City and County, 2020),https://oag.ca.gov/sites/default/files/People%20v.%20Glow%20-%20Final%20Judgment%20and%20Permanent%20Injunction%20-%2007374856.pdf.

privileged-access management solution; restricting and monitoring the creation of new accounts and ensuring that their access and privileges are limited as set forth in subsections (b)(2)(D)(i)–(ii); and restricting and monitoring physical access to personal information; (5) inventory and management of personal information and the business's information system, including inventories and classification and tagging of personal information; hardware and software inventories and the use of allowlisting; hardware and software approval processes and preventing the connection of unauthorized hardware and devices to the business's information system; (6) secure configuration of hardware and software, including software updates and upgrades; securing on-premises and cloud-based environments; masking the sensitive personal information set forth in Civil Code section 1798.145, subdivisions (ae)(1)(A) and (B) and other personal information as appropriate by default in applications; security patch management; and change management; (7) internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting; (8) audit-log management, including the centralized storage, retention, and monitoring of logs; (9) network monitoring and defenses, including the deployment of bot-detection and intrusion-detection and intrusion-prevention systems, and data-loss-prevention systems; (10) antivirus and antimalware protections; (11) segmentation of an information system; (12) limitation and control of ports, services, and protocols; (13) cybersecurity awareness, education, and training, including training for each employee, independent contractor, and any other personnel to whom the business provides access to its information system; and how the business maintains current knowledge of changing cybersecurity threats and countermeasures; (14) secure development and coding best practices, including code-reviews and testing; (15) oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053; (16) retention schedules and proper disposal of personal information no longer required to be retained by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means; (17) how the business manages its responses to security incidents, which are defined for purposes of the subsection as "an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of the business's information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of the business's cybersecurity program. Unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information is a

security incident" (i.e., its incident response management), including documentation of its incident response plan, and how the business tests its incident-response capabilities; and (18) the business's business-continuity and disaster-recovery plans, including data-recovery capabilities and backups.

The purpose of this subsection is to implement and operationalize the requirement that businesses complete annual cybersecurity audits, and it is necessary to fulfill the Agency's obligation to establish a process to ensure that audits are thorough and to define the scope of the audit. It provides clarity and guidance for businesses, their auditors, and consumers about how businesses must complete a thorough cybersecurity audit. These 18 components reflect common recommendations and requirements for businesses to defend their information systems and the personal information they process. Each of the components included within subsection (b)(2) — as well as the examples of how businesses often implement them — align with the guidance provided in prominent cybersecurity frameworks and resources, such as the NIST Cybersecurity Framework, the Center for Internet Security Critical Security Controls ("CSC"), and guidance from the FTC and the Attorney General.[29]

---

[29] *See, e.g.,* NAT'L INST. OF STANDARDS & TECH., NIST CYBERSECURITY FRAMEWORK (CSF) VERSION 2.0 (Feb. 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf; CTR. FOR INTERNET SEC., THE CIS CONTROLS (version 8), https://www.cisecurity.org/controls; Alex Gaynor, *Security Principles: Addressing Underlying Causes of Risk in Complex Systems*, FED. TRADE COMM'N (Feb. 1, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems; FED. TRADE COMM'N, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS (Feb. 2021), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business; FED. TRADE COMM'N, CAREFUL CONNECTIONS: KEEPING THE INTERNET OF THINGS SECURE (Sept. 2020), https://www.ftc.gov/business-guidance/resources/careful-connections-keeping-internet-things-secure; FED. TRADE COMM'N, MOBILE SECURITY UPDATES: UNDERSTANDING THE ISSUES (Feb. 2018), https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf; *Stick with Security: A Business Blog Series*, FED. TRADE COMM'N: BUS. BLOG (Oct. 2017), https://www.ftc.gov/business-guidance/privacy-security/stick-with-security-business-blog-series; Thomas B. Pahl, *Stick with Security: Secure* Paper*, Physical Media, and Devices*, FED. TRADE COMM'N: BUS. BLOG (Sept. 29, 2017), https://www.ftc.gov/business-guidance/blog/2017/09/stick-security-secure-paper-physical-media-and-devices; Thomas B. Pahl, *Stick with Security: Put Procedures in Place to Keep Your Security Current and Address Vulnerabilities that may Arise*, FED. TRADE COMM'N: BUS. BLOG (Sept. 22, 2017), https://www.ftc.gov/business-guidance/blog/2017/09/stick-security-put-procedures-place-keep-your-security-current-and-address-vulnerabilities-may-arise; Thomas B. Pahl, *Stick with Security: Make Sure Your Service Providers Implement Reasonable Security Measures*, FED. TRADE COMM'N: BUS. BLOG (Sept. 15, 2017), https://www.ftc.gov/business-guidance/blog/2017/09/stick-security-make-sure-your-service-providers-implement-reasonable-security-measures; Thomas B. Pahl, *Stick with*

In 2016, the Attorney General described the CSC as "a consensus list of the best defensive controls to detect, prevent, respond to, and mitigate damage from cyber attacks" and stated that "failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."[30] Therefore, it is necessary for a thorough cybersecurity audit to identify, assess, and document each of the 18 components of the business's cybersecurity program, as applicable; and if not applicable, to document why the component isn't necessary to protect consumers' personal information and how the safeguards the business has in place provide at least equivalent security.

For example, subsection (b)(2)(D)(i)(1) explains how businesses may implement account management and access controls, by restricting their employees' privileges and access to personal information to just what those employees need to

---

Security: Apply Sound Security Practices When Developing New Products, FED. TRADE COMM'N.: BUS. BLOG (Sept. 8, 2017), https://www.ftc.gov/business-guidance/blog/2017/09/stick-security-apply-sound-security-practices-when-developing-new-products; Thomas B. Pahl, *Stick with Security: Secure Remote Access to Your Network*, FED. TRADE COMM'N.: BUS. BLOG (Sept. 1, 2017), https://www.ftc.gov/business-guidance/blog/2017/09/stick-security-secure-remote-access-your-network; Thomas B. Pahl, *Stick with Security: Segment Your Network and Monitor Who's Trying to Get In and Out*, FED. TRADE COMM'N: BUS. BLOG (Aug. 25, 2017), https://www.ftc.gov/business-guidance/blog/2017/08/stick-security-segment-your-network-and-monitor-whos-trying-get-and-out; Thomas B. Pahl, *Stick with Security: Store Sensitive Personal Information Securely and Protect It During Transmission*, FED. TRADE COMM'N.: BUS. BLOG (Aug. 18, 2017), https://www.ftc.gov/business-guidance/blog/2017/08/stick-security-store-sensitive-personal-information-securely-and-protect-it-during-transmission; Thomas B. Pahl, *Stick with Security: Require Secure Passwords and Authentication*, FED. TRADE COMM'N.: BUS. BLOG (Aug. 11, 2017), https://www.ftc.gov/business-guidance/blog/2017/08/stick-security-require-secure-passwords-and-authentication; Thomas B. Pahl, *Stick with Security: Control Access to Data Sensibly*, FED. TRADE COMM'N.: BUS. BLOG (Aug. 4, 2017), https://www.ftc.gov/business-guidance/blog/2017/08/stick-security-control-access-data-sensibly; Thomas B. Pahl, *Start with Security – and Stick With It*, FED. TRADE COMM'N.: BUS. BLOG (Jul. 28, 2017), https://www.ftc.gov/business-guidance/blog/2017/07/start-security-and-stick-it; *App Developers: Start with Security*, FED. TRADE COMM'N.: BUS. BLOG (May 2017), https://www.ftc.gov/business-guidance/resources/app-developers-start-security; *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business; FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; KAMALA D. HARRIS, ATTORNEY GENERAL, CALIFORNIA DATA BREACH REPORT 30 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf; KAMALA D. HARRIS, ATTORNEY GENERAL, CYBERSECURITY IN THE GOLDEN STATE (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/2014_cybersecurity_guide.pdf?.

[30] KAMALA D. HARRIS, ATTORNEY GENERAL, CALIFORNIA DATA BREACH REPORT 30 (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

perform their job functions, and by revoking those privileges and access when they're no longer required, including with employees are terminated. This is necessary to illustrate how businesses control access to personal information. These subsections and their examples are necessary to provide clarity regarding key components of a business's cybersecurity program. These examples benefit businesses, their auditors, and consumers by providing guidance regarding the kinds of practices that provide protections for consumers' personal information and the kinds of practices that auditors may prioritize in their assessment and documentation**.**

Subsection (b)(3) requires the audit to describe how the business implements and enforces compliance with the applicable components set forth in subsections (b)(1) and (b)(2), including the safeguards identified in the business's cybersecurity policies and procedures. Policies, procedures, and other safeguards will not provide their intended protections unless they are consistently implemented and enforced. This subsection is necessary to clarify that implementing and enforcing compliance with policies, procedures, and other safeguards is critical to how a business protects consumers' personal information and must therefore be included as part of a thorough cybersecurity audit.

Subsection (b)(4) clarifies that nothing in section 7123 prohibits an audit from assessing and documenting components of a cybersecurity program that are not set forth in subsections (b)(1)–(2). It benefits businesses, their auditors, and consumers by providing flexibility for businesses and their auditors to assess and evaluate additional components that the regulations do not explicitly list but that may be part of how the business protects consumers' personal information. This subsection is necessary to ensure that businesses and their auditors understand that the business's cybersecurity audit is not restricted to the components listed in subsections (b)(1)–(2).

Subsections (c)(1)–(5) provide clarity and guidance for businesses and their auditors regarding how to ensure the business's audit is thorough, by ensuring that the audit assesses the effectiveness, gaps, and weaknesses in the business's cybersecurity program, and by building in assurances of accountability for the business's cybersecurity program. This subsection is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and to define the scope of the audit. It also ensures a baseline of consistent audit content.

More specifically, **subsection (c)(1)** requires an audit to assess and document how effective the business's cybersecurity program components are at protecting consumers' personal information. **Subsections (c)(2)–(3)** require the audit to identify and describe the gaps or weaknesses in those components, and to document the business's plan to address those gaps and weaknesses. Collectively, these are key pieces of information that a business would need to prioritize and remediate vulnerabilities that put consumers' personal information at risk and enable the business to resolve those vulnerabilities. These subsections are necessary to clarify for businesses and their auditors what must be included in a thorough audit, by clarifying that it must include the effectiveness of its components, the gaps and weaknesses therein, and the business's plan to resolve those gaps and weaknesses.

Subsections (c)(4)–(5) require the audit to include the titles of individuals responsible for the business's cybersecurity program; and the date that the program and any evaluations of it were presented to the business's board, governing body, or — if neither of those exists — to the business's highest-ranking executive responsible for the program. Together with subsections (c)(1)–(3), these requirements create accountability for those responsible for the business's cybersecurity program. In addition, the details required by this subsection benefit businesses, their auditors, and consumers by helping successive auditors understand the business's cybersecurity posture over time, especially when the business engages different auditors from one year to the next and when there is turnover within the business of those responsible for the business's cybersecurity program.

Subsections (d) and **(e)** require the audit to include a include a sample copy, or a description, of two kinds of notifications, as detailed below. These subsections are necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and to define the scope of the audit. They require audits to include specific evidence of the kinds of gaps and weaknesses in a business's cybersecurity program that must be included in a cybersecurity audit. These subsections, together with subsections 7122(h) and (i), ensure that the most senior people in the business responsible for its cybersecurity program will be made aware of this evidence and how it fits into the business's cybersecurity posture. These subsections also benefit businesses, their auditors, and consumers by providing clear guidance and ensuring a baseline of consistent audit content.

Specifically, **subsection (d)** requires the audit to include a sample copy, or a description, of any notification to a consumer that was required by Civil Code section 1798.82, subdivision (a). That subdivision of the Civil Code requires a business to disclose certain information to a consumer if certain personal information is reasonably believed to have been acquired by an unauthorized person. The information a business would have to disclose includes a plain language description of what happened, the information involved, what the business is doing, and what the consumer can do. (*See* Civ. Code, § 1798.82, subd. (d).) The details provided in this subsection ensure that the audit takes into account the instances of unauthorized access to consumers' personal information that were significant enough to trigger Civil Code section 1798.82, subdivision (a)'s breach-notification requirement. Such breaches evidence the kinds of gaps and weaknesses in a business's cybersecurity program that must be included in a cybersecurity audit. (*See* subsections 7122(e)(2)–(3), 7123(c)(2)–(3).)

Subsection (e) requires the audit to include a sample copy, or a description, of any notification to any agency with jurisdiction over privacy laws or other data processing authority in California, other states, territories, or countries of unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information, as well as the dates and details of the activity that gave rise to the required notifications and any related remediation measures taken by the business. The details required by this subsection ensure that the audit takes into account the instances of unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information that were significant enough to trigger notification to other agencies or data-processing authorities. Such instances evidence the kinds of gaps and weaknesses in a business's cybersecurity program that must be included in a cybersecurity audit. (*See* subsections 7122(e)(2)–(3), 7123(c)(2)–(3).)

Subsection (f) clarifies that if a business has engaged in a cybersecurity audit, assessment, or evaluation that meets all of the requirements of Article 9, the business is not required to complete a duplicative cybersecurity audit, but the business must specifically explain how what it has already done meets all of the regulatory requirements. This subsection also clarifies that if what the business has done does not meet all of the requirements of Article 9, the business must supplement it with additional information required to meet all such requirements. This subsection is necessary to clarify that businesses can leverage cybersecurity

audits, assessments, or evaluations that they have engaged in for other purposes to help meet their obligations under Article 9. It provides flexibility and reduces the burden on businesses,[31] while ensuring that cybersecurity audits consistently meet the requirements in Article 9.

§ 7124. Certification of Completion.

The purpose of section 7124 is to provide clarity and guidance to businesses about what they must submit to the Agency regarding their cybersecurity audits and when they must submit it. Together with Article 9's substantive requirements, this section provides an assurance of, and accountability for, the thoroughness and independence of the business's audit. This section is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and independent. It is informed by practices in other contexts, such as FTC orders and the NYDFS Cybersecurity Regulations,[32] and is consistent with the purpose and intent of the CCPA to further protect consumers' privacy, which necessarily includes further protecting their personal information. (*See* Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3.)

Specifically, **subsection (a)** requires each business that is required to complete a cybersecurity audit to submit to the Agency every calendar year a written certification that the business completed the cybersecurity audit as set forth in Article 9.

Subsection (b) requires the business to submit its written certification to the Agency through https://cppa.ca.gov/ and identify the 12 months that the audit covers.

Subsections (a) and **(b)** together provide flexibility for businesses as to when during the calendar year they submit their certification, while clarifying that the certification must identify the 12 months covered by the audit. These subsections are necessary to provide clarity and guidance for businesses and consumers about

---

[31] *See California Consumer Privacy Act Regulations, Pre-Rulemaking Informational Sessions*, Transcript at 65, CAL. PRIV. PROT. AGENCY (Mar. 30, 2022), *available at* https://cppa.ca.gov/meetings/materials/20220330_transcript.pdf.

[32] *See, e.g.,* Final Decision and Order at 10, Blackbaud, Inc., FTC Docket No. C-4804 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2023181_blackbaud_final_consent_package.pdf; N.Y. COMP. CODES R. & REGS. tit. 23, § 500.0.

what businesses must submit to the Agency, when, and how. Together with subsections 7121(a) and (b), they reduce the burden on businesses while ensuring that there are no gaps in the months covered by successive audits, and that there is a certification covering all 12 months of each audit, consistent with the intent and purpose of the statute to protect consumers' privacy.

Subsection (c) requires the business's written certification to the Agency to be signed and dated by a member of the business's board, governing body, or—if neither of those exists—to the business's highest-ranking executive with authority to certify on behalf of the business and who is responsible for oversight of the business's cybersecurity-audit compliance. It also requires that the written certification include a statement certifying that the signer has reviewed and understands the findings of the cybersecurity audit, and that the signer include their name and title. Together with the requirements in subsections 7122(h) and (i)—that the most senior individuals in the business be informed about the business's cybersecurity posture through its audit results—this subsection ensures that the most senior individuals in the business are accountable for the business's compliance with the cybersecurity audit requirements. Board involvement and accountability for cybersecurity results in more attention and resources being dedicated to cybersecurity and the protection of consumers' personal information; it is also consistent with cybersecurity and auditing approaches in other frameworks, such as the NYDFS Cybersecurity Regulations.[33] This subsection is necessary to fulfill the Agency's statutory mandate to establish a process to ensure that audits are thorough and independent and to further the intent and purpose of the CCPA to protect consumers' privacy.

ARTICLE 10. RISK ASSESSMENTS

Civil Code section 1798.185, subdivision (a)(15)(B), requires the Agency to issue regulations requiring that businesses conduct risk assessments when their processing of personal information presents significant risk to consumers' privacy. It also requires the Agency to issue regulations requiring that businesses submit these risk assessments to the Agency on a regular basis.

The purpose of Article 10 is to operationalize the CCPA's statutory requirement to issue regulations. As explained further in the sections below, these regulations are

[33] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.17(b)(2); *see also supra* note 25.

necessary to provide clarity and specificity to implement the law's risk-assessment requirements for businesses. These regulations will benefit both businesses and consumers by creating clear rules regarding when and how a risk assessment must be conducted, and how a risk assessment must be submitted to the Agency. This Article is informed by the purpose and intent set forth in the CCPA, public comments received by the Agency during preliminary rulemaking activities, academic scholarship, existing privacy frameworks, and observations in the current marketplace.

§ 7150. When a Business Must Conduct a Risk Assessment.

The purpose of section 7150 is to specify when businesses' processing of consumers' personal information presents significant risk to consumers' privacy and requires a risk assessment.

Subsections (a) and **(b)** collectively restate and operationalize the statutory requirement in Civil Code section 1798.185, subdivision (a)(15)(B), that businesses conduct a risk assessment when their processing of consumers' personal information presents significant risk to consumers' privacy. **Subsection (a)** restates the statutory language and cross-references **subsection (b)**, which explains when businesses' processing presents significant risk to consumers' privacy. **Subsections (a)** and **(b)** are necessary to clarify for businesses when their processing presents significant risk to consumers' privacy and, therefore, when they must conduct a risk assessment. They benefit businesses by providing a clear standard for when they must conduct a risk assessment, and benefit consumers by ensuring that businesses conduct a risk assessment prior to engaging in the enumerated processing activities using their personal information.

Subsection (b)(1) identifies selling or sharing personal information as a significant risk to consumers' privacy requiring a risk assessment. This subsection is necessary because selling and sharing personal information presents several significant risks to consumers' privacy, such as impairing consumers' control of their personal information, imposing economic costs on consumers (e.g., through predatory advertising to vulnerable populations, such as the elderly), and creating opportunities for criminal activity, such as stalking, harassment, physical violence,

phishing and other scams, and identity theft.[34] This requirement also works to harmonize the application of California law with other privacy frameworks that require risk assessments for processing activities that present a heightened risk of harm to a consumer. Fifteen other states generally require a risk assessment prior to selling personal information or sharing that information for targeted

[34] *See, e.g.*, Byron Tau, *Antiabortion Group Used Cellphone Data to Target Ads to Planned Parenthood Visitors*, WALL STREET JOURNAL (May 18, 2023), https://www.wsj.com/articles/antiabortion-group-used-cellphone-data-to-target-ads-to-planned-parenthood-visitors-446c1212; Office of the Privacy Comm'r of Canada, *Investigation into Home Depot of Canada Inc.'s Compliance with PIPEDA* (Jan. 26, 2023), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2023/pipeda-2023-001/; Jon Keegan & Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, THE MARKUP (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you; Samantha Lai & Brooke Tanner, *Examining the Intersection of Data Privacy and Civil Rights*, BROOKINGS INST. (July 18, 2022), https://www.brookings.edu/articles/examining-the-intersection-of-data-privacy-and-civil-rights/; Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FED. TRADE COMM'N.: BUS. BLOG (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal; Justin Sherman, *How Shady Companies Guess Your Religious, Sexual Orientation, and Mental Health*, SLATE (Apr. 26, 2023), https://slate.com/technology/2023/04/data-broker-inference-privacy-legislation.html; Zack Whittaker, *Alcohol Recovery Startups Monument and Tempest Shared Patients' Private Data with Advertisers*, TECH CRUNCH (Apr. 4, 2023), https://techcrunch.com/2023/04/04/monument-tempest-alcohol-data-breach/; Muhammad Ali et al., *Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes*, 3 PROC. OF THE ACM ON HUM.-COMPUT. INTERACTION, 1 (Nov. 2019), https://doi.org/10.1145/3359301; Lesley Fair, *First FTC Health Breach Notification Rule Case Addresses GoodRx's Not-So-Good Privacy Practices*, FED. TRADE COMM'N.: BUS. BLOG (Feb. 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices; Brian Boynton, Principal Deputy Assistant Att'y Gen., Remarks at White House Roundtable on Protecting Americans from Harmful Data Broker Practices (Aug. 15, 2023; Press Release, FED. TRADE COMM'N, FTC Charges Data Brokers with Helping Scammer Take More Than $7 Million from Consumers' Accounts (Aug. 12, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/08/ftc-charges-data-brokers-helping-scammer-take-more-7-million-consumers-accounts; Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, DUKE SANFORD CYBER POL'Y PROGRAM (2021) [hereinafter *Data Brokers and Sensitive Data*]; Marshall Allen, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates*, NPR (July 17, 2018), https://www.npr.org/sections/health-shots/2018/07/17/629441555/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

advertising.[35] Similarly, selling or sharing personal information is consistent with the risk factors that would require a data protection impact assessment under the European Union's GDPR.[36]

Subsection (b)(2) identifies processing sensitive personal information as a significant risk to consumers' privacy requiring a risk assessment. This subsection is necessary because processing sensitive personal information presents several significant risks to consumers' privacy:

- Misuse of sensitive personal information can enable harassment and stalking.[37] In addition, if this information is leaked, such as through a data breach, it can lead to serious privacy harm to consumers, including through revealing their health and genetic information to unauthorized third parties.[38]

---

[35] *See, e.g.*, COLO. REV. STAT. § 6-1-1309(2)(a)-(b) (2021); CONN. GEN. STAT. § 42-522 (2023); 6 DEL. CODE ANN. tit. 6, 12D, § 108(a)(1)-(2) (2024); IND. CODE § 24-15-6-1(b)(1)-(2) (2023); KY. REV. STAT. § 367.6(1)(a)-(b) (2024); Maryland Online Data Privacy Act of 2024, S.B. 541, 2004 Gen. Assemb., Reg. Sess. § 14-4601(A)(1)-(2) (2024); MINN. STAT. § 3250.08(b)(1)-(2) (2024); MONT. CODE § 30-14-2814 (2024); NEB. L.B. 1074, 108th LEG. § 16(1)(a)-(b) (2024); N.H. REV. STAT. § 507-H:8(I)(a)-(b) (2024); N.J. STAT. ANN. § 56:8-166.12(c)(1)-(2) (2023); OR. REV. STAT. § 646A.586(1)(b)(A)-(B) (2023);TENN. CODE ANN. § 47-18-3206(a)(1)-(2) (2024); TEX. BUS. & COM. CODE § 541.105(a)(1)-(2) (2023); VA. CODE § 59.1-580(A)(1)-(2) (2021).

[36] *See* Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679*, Sec. III(B)(a) (2017) [hereinafter DPIA Guidelines].

[37] Press Release, MASS. OFF. OF THE ATT'Y GEN., AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities, (Apr. 4, 2017), https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities; Cohen, *supra* note 34.

[38] Sara Morrison, *GoodRx Made Money Off Your Health Data. The FTC Is Making It Pay*, VOX (Feb. 1, 2023), https://www.vox.com/recode/23581260/goodrx-ftc-privacy; Whittaker, *supra* note 34; Zack Whittaker, *Telehealth Startup Cerebral Shared Millions of Patients' Data with Advertisers*, TECH CRUNCH (Mar. 10, 2023), https://techcrunch.com/2023/03/10/cerebral-shared-millions-patient-data-advertisers/; Lorenzo Franceschi-Bicchierai & Zack Whittaker, *23andMe Says Hackers Accessed 'Significant Number' of Files about Users' Ancestry*, TECH CRUNCH (Dec. 1, 2023), https://techcrunch.com/2023/12/01/23andme-says-hackers-accessed-significant-number-of-files-about-users-ancestry/; Piers Gooding & Timothy Kariotis, *Mental Health Apps Are Not Keeping Your Data Safe*, SCI. AM. (Nov. 15, 2022), https://www.scientificamerican.com/article/mental-health-apps-are-not-keeping-your-data-safe/; Zack Whittaker, *Mr. Cooper Hackers Stole Personal Data on 14 Million Customers*, TECH CRUNCH (Dec. 28, 2023), https://techcrunch.com/2023/12/18/mr-cooper-hackers-stole-

- Processing this information also can impair consumers' control over their personal information, impose economic costs on consumers, and cause psychological and reputational harm (e.g., emotional distress resulting from the disclosure of consumers' health information or use of this information for non-medical purposes).[39]

- Sensitive personal information also can be used to facilitate discrimination based on protected characteristics.[40]

- Lastly, processing sensitive personal information presents unique privacy risks for consumers because one type of sensitive personal information can reveal other sensitive details about them. For example, the collection of a consumer's precise geolocation information can reveal visits to drug addiction or psychological facilities, religious centers, reproductive care

---

personal-data-on-14-million-customers/; Zack Whittaker, *Healthcare Giant McLaren Reveals Data on 2.2 million Patients Stolen During Ransomware Attack*, TECH CRUNCH (Nov. 13, 2023), https://techcrunch.com/2023/12/18/mr-cooper-hackers-stole-personal-data-on-14-million-customers/.

[39] *See, e.g.*, Alexandrine Royer, *The Wellness Industry's Risky Embrace of AI-Driven Mental Health Care*, BROOKINGS INST. (Oct. 14, 2021), https://www.brookings.edu/articles/the-wellness-industrys-risky-embrace-of-ai-driven-mental-health-care/; Stuart A. Thompson & Charlie Warzel, *Smartphones Are Spies. Here's Whom They Report To*, N.Y. TIMES (Dec. 20, 2019), https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html; Thomas Germain, *Mental Health Apps Aren't All as Private as You May Think*, CONSUMER REPS. (Mar. 2, 2021), https://www.consumerreports.org/health/health-privacy/mental-health-apps-and-user-privacy-a7415198244/; *ICO Orders Serco Leisure to Stop Using Facial Recognition Technology to Monitor Attendance of Leisure Centre Employees*, UK INFO. COMM'R'S OFFICE (Feb. 23, 2024), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-orders-serco-leisure-to-stop-using-facial-recognition-technology/; Umar Iqbal et al., *Your Echoes Are Heard: Tracking, Profiling, and Ad Targeting in the Amazon Smart Speaker Ecosystem* (May 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Iqbal-Bahrami-Trimananda-Cui-Garrido-Dubois-Choffnes-Markopoulou-Roesner-Shafq-Your-Echos-are-Heard.pdf; Keith Pocard, *The Real Harm of Crisis Text Line's Data Sharing*, WIRED (Feb. 1, 2022), https://www.wired.com/story/consumer-protections-data-services-care/; Allen, *supra* note 34; Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, THE MIT PRESS READER (Jan. 14, 2021), https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/; Kashmir Hill & Aaron Krolik, *At Talkspace, Start-Up Culture Collides with Mental Health Concerns*, N.Y. TIMES (Aug. 7, 2020), https://www.nytimes.com/2020/08/07/technology/talkspace.html.

[40] *Data Brokers and Sensitive Data*, *supra* note 34; Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.

centers, and political rallies, which presents a risk to consumers' willingness to visit these facilities and can chill their exploration of ideas.[41]

This subsection also works to harmonize the application of California law with fifteen other state privacy laws that require risk assessments when processing sensitive personal information, as well as with the European Union's GDPR.[42]

Subsection (b)(2)(A) exempts from the risk-assessment requirements the processing of sensitive personal information for 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. This subsection also explains that any other processing of consumers' sensitive personal information is subject to the risk-assessment requirements. This requirement incorporates feedback received during preliminary rulemaking activities and is necessary to limit the risk-assessment burden on businesses for processing of sensitive personal information that is required by law, such as certain wage reporting, or that is limited to routine personnel activities raised by public comments, such as administering compensation payments. It also is necessary to clarify that processing sensitive personal information of consumers, which includes employees and independent contractors, outside of these activities would still require a risk assessment.

Subsection (b)(3) identifies using ADMT for a significant decision concerning a consumer or for extensive profiling as a significant risk to consumers' privacy requiring a risk assessment. **Subsection (b)(3)(A)** defines the term "significant decision" to mean a decision that results in access to, or the provision or denial of, certain goods and services. These goods and services are: financial or lending

---

[41] Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html; Geoffrey A. Fowler, *Google Promised to Delete Sensitive Data. It Logged My Abortion Clinic Visit*, WASH. POST (May 9, 2023), https://www.washingtonpost.com/technology/2023/05/09/google-privacy-abortion-data/; Lai & Tanner, *supra* note 34.

[42] *See, e.g.*, COLO. REV. STAT. § 6-1-1309(2)(c); CONN. GEN. STAT. § 42-522; 6 DEL. CODE ANN. tit. 6, 12D, § 108(a)(4); IND. CODE § 24-15-6-1(b)(4); KY. REV. STAT. § 367.6(1)(d); Maryland Online Data Privacy Act of 2024, S.B. 541, 2004 Gen. Assemb., Reg. Sess. § 14-4610(A)(3); MINN. STAT. § 3250.08(b)(3); MONT. CODE § 30-14-2814(1)(d); NEB. L.B. 1074, 108th LEG. § § 16(1)(d); N.H. REV. STAT. § 507-H:8(I)(d); N.J. STAT. ANN. § 56:8-166.12(c)(3)); OR. REV. STAT. § 646A.586(1)(b)(B); TENN. CODE ANN. § 47-18-3206(a)(4); TEX. BUS. & COM. CODE § 541.105(a)(4) ; VA. CODE § 59.1-580(A)(4). *See also* DPIA Guidelines, *supra* note 36, at Sec. III(B)(a).

services; housing; insurance; education enrollment or opportunity; criminal justice; employment or independent contracting opportunities or compensation; healthcare services; or essential goods or services.

It also states the types of education enrollment or opportunities that are in scope of the regulation, specifically admission or acceptance into academic or vocational programs; educational credentials; and suspension and expulsion. Similarly, the subsection states the types of employment or independent contracting opportunities that are within scope of the regulation, specifically hiring; allocation/assignment of work and compensation; promotion; and demotion, suspension, and termination.

Lastly, this subsection explains that "significant decisions" include only decisions using information that is not subject to relevant data-level exceptions in the CCPA.

Subsection (b)(3)(B) defines the term "extensive profiling" to address profiling consumers in work and educational contexts, in public, or for behavioral advertising.

Subsection (b)(3) is necessary because using ADMT for a significant decision or for extensive profiling presents significant risk to consumers' privacy, such as discrimination based on different protected classes, lack of consumer control over their personal information, and psychological and reputational harm from invasive surveillance.[43] Academic scholarship and news reports identify several privacy risks stemming from these uses of ADMT, such as:

---

[43] *See, e.g.*, Rebecca Kelly Slaughter, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 YALE J.L. & TECH. (2021); Annette Bernhardt et al., *The Data-Driven Workplace and the Case for Worker Technology Rights*, ILR REVIEW (Jan. 2023); Jessica Vitak & Michael Zimmer, *Surveillance and the Future of Work: Exploring Employees' Attitudes Toward Monitoring in a Post-COVID Workplace*, J. OF COMPT.-MEDIATED COMMC'N. (2023); Brian Fung, *How Stores Use Your Phone's Wifi to Track Your Shopping Habits*, WASH. POST (Oct. 19, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits/; Robert Channick, *Macy's Hit with Privacy Lawsuit Over Alleged Use of Controversial Facial Recognition Software*, CHI. TRIB. (Aug. 11, 2020), https://www.chicagotribune.com/2020/08/11/macys-hit-with-privacy-lawsuit-over-alleged-use-of-controversial-facial-recognition-software/; ANDREAS CLAESSON & TOR E. BJØRSTAD, NORWEGIAN CONSUMER COUNCIL, "OUT OF CONTROL" — A REVIEW OF DATA SHARING BY POPULAR MOBILE APPS (2020), Consumer Council, Out of Control 19 (2020); *Profiling by Powerful Tech Firms Risks Undermining Consumer Choice*, UNIV. OF OXFORD: NEWS & EVENTS (May 28, 2021), https://www.ox.ac.uk/news/2021-05-28-profiling-powerful-tech-firms-risks-undermining-consumer-choice-oxford-research; Jose Gonzalez Cabanas et al., *Facebook Use of Sensitive Data for Advertising in Europe* (Feb. 14, 2018), https://arxiv.org/pdf/1802.05030.

- The use of ADMT to monitor, discipline, and terminate employees can harm their physical and mental health, risk leakage of their sensitive personal information (e.g., an employee's pregnancy or sexual orientation), lead to surveillance of workers' union activity, discriminate based on consumers' disabilities, and lead to diminished worker safety. Reports also indicate that these uses of ADMT can at times have no positive — and even harmful — effects on employees' performance at work and safety.[44]

- Similarly, educational profiling has raised concerns about the use of students' race for predictive risk-scoring and for targeted advertising by educational institutions, stigmatization as a result of misidentification of students as a potential danger to others, and a lack of transparency for

[44] *See, e.g.*, Kate Morgan & Delaney Nolan, *How Worker Surveillance Is Backfiring on Employers*, BBC (Jan. 30, 2023), https://www.bbc.com/worklife/article/20230127-how-worker-surveillance-is-backfiring-on-employers; Chase Thiel et al., *Monitoring Employees Makes Them More Likely to Break Rules*, HARVARD BUS. REV. (June 27, 2022), https://hbr.org/2022/06/monitoring-employees-makes-them-more-likely-to-break-rules; Karen Levy, *Surveillance Was Supposed to Make Long-Haul Trucking Safer. Did It?*, SLATE (Dec. 6, 2022), https://slate.com/technology/2022/12/data-driven-trucker-surveillance-fatigue-elds.html; Zoe Corbyn, *'Bossware Is Coming for Almost Every Worker': The Software You Might Not Realize Is Watching You*, THE GUARDIAN (Apr. 22, 2022), https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic; Annie Palmer, *Amazon Uses an App Called Mentor to Track and Discipline Delivery Drivers*, CNBC (Feb. 12, 2021), https://www.cnbc.com/2021/02/12/amazon-mentor-app-tracks-and-disciplines-delivery-drivers.html; Benjamin Wiseman, Remarks at the Harvard Journal of Law & Technology on Worker Surveillance & AI (Feb. 8, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Jolt-2-8-24-final.pdf; Alex Engler, *For Some Employment Algorithms, Disability Discrimination by Default*, BROOKINGS INST. (Oct. 31, 2019), https://www.brookings.edu/articles/for-some-employment-algorithms-disability-discrimination-by-default/; Jo Constantz, *'They Were Spying On Us': Amazon, Walmart, Use Surveillance Technology to Bust Unions*, NEWSWEEK (Dec. 13, 2021), https://www.newsweek.com/they-were-spying-us-amazon-walmart-use-surveillance-technology-bust-unions-1658603; Annette Bernhardt, Reem Suleiman, & Lisa Kresge, *Data and Algorithms at Work: The Case for Worker Technology Rights*, UC BERKELEY LABOR CENTER (Nov. 3, 2021), https://laborcenter.berkeley.edu/data-algorithms-at-work/#s-12; Nathan Newman, *Reengineering Workplace Bargaining: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in The Workplace*, 85 U. OF CINN. L. REV. 693, 695 (2017); Hayley Peterson, *Amazon-owned Whole Foods Is Quietly Tracking Its Employees with a Heat Map Tool That Ranks Which Stores Are Most at Risk of Unionizing*, BUSINESS INSIDER (Apr. 20, 2020), https://www.businessinsider.com/whole-foods-tracks-unionization-risk-with-heat-map-2020-1.

students and their parents about how their personal information will be collected and used.[45]

- In the context of public profiling, the use of facial recognition technology for fraud prevention that is improperly deployed can cause subsequent stigmatization for consumers due to false accusations of wrongdoing and psychological stress from improper searches and wrongful arrest.[46] Equally concerning is that people of color and women appear to be at increased risk of these harms, because they are more likely to be incorrectly matched by facial-recognition technologies.[47]

- There also is a significant risk of discrimination when using ADMT for profiling for behavioral advertising. For example, advertisements for high-paying job opportunities on large platforms have been served disproportionately to men. In another case, real estate advertisers used social media platforms to target housing advertisements based on protected classes, such as race, gender, and age.[48]

Subsection (b)(3)(A) is necessary to clarify which "significant decisions" are in scope of the proposed regulations, specifically decisions that have important

---

[45] *See, e.g.*, Todd Feathers, *College Prep Software Naviance Is Selling Advertising Access to Millions of Students*, THE MARKUP (Jan. 13, 2022), https://themarkup.org/machine-learning/2022/01/13/college-prep-software-naviance-is-selling-advertising-access-to-millions-of-students; Todd Feathers, *This Private Equity Firm Is Amassing Companies That Collect Data on America's Children*, THE MARKUP (Jan. 11, 2022), https://themarkup.org/machine-learning/2022/01/11/this-private-equity-firm-is-amassing-companies-that-collect-data-on-americas-children; National Association of Secondary School Principals, *Position Statement: Student Profiling*, NASSP, https://www.nassp.org/top-issues-in-education/position-statements/student-profiling/.

[46] *See, e.g.*, Office of the Information & Privacy Commissioner for British Columbia, *Canadian Tire Association Dealers' Use of Facial Recognition Technology* (Apr. 2023); Lesley Fair, *Coming Face to Face with Rite Aid's Allegedly Unfair Use of Facial Recognition Technology*, FED. TRADE COMM'N.: BUS. BLOG (Dec. 19, 2023), https://www.ftc.gov/business-guidance/blog/2023/12/coming-face-face-rite-aids-allegedly-unfair-use-facial-recognition-technology; Johana Bhuiyan, *Facial Recognition Used After Sunglass Hut Robbery Led to Man's Wrongful Jailing, Says Suit*, THE GUARDIAN (Jan. 22, 2024), https://www.theguardian.com/technology/2024/jan/22/sunglass-hut-facial-recognition-wrongful-arrest-lawsuit.

[47] *See* Fair, *supra* note 46.

[48] Alex P. Miller & Kartik Hosanagar, *How Targeted Ads and Dynamic Pricing Can Perpetuate Bias*, HARVARD BUS. REV. (Nov. 8, 2019), https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias.

consequences for consumers. This subsection is necessary to clarify that "significant decisions" include only decisions using information that is not subject to relevant data-level exceptions in the CCPA, to avoid confusion about how the definition of "significant decision" interacts with the CCPA's exceptions for certain health, credit, and financial information (which are subject to other privacy laws' protections). **Subsection (b)(3)(B)** is necessary to clarify which uses of ADMT for extensive profiling require a risk assessment, specifically those that are likely to cause significant harm to consumers, as discussed above. This subsection also works to harmonize the application of California law with privacy frameworks in fifteen other U.S. states as well as in the European Union, which require risk assessments for processing that presents a heightened risk of harm to a consumer, including profiling that poses a reasonably foreseeable risk of substantial injury, that is carried out for the purpose of systematic monitoring of employees' activities, or that uses systematic monitoring of publicly available places.[49]

Subsection (b)(4) identifies processing of personal information to train ADMT or AI that is capable of being used for a significant decision, to establish individual identity, for physical or biological identification or profiling, for the generation of a deepfake, or for the operation of generative models, as a significant risk to consumers' privacy requiring a risk assessment. This subsection is necessary because these training uses of ADMT and AI present significant risks to consumers' privacy, including data leakage that can reidentify consumers whose personal information was used to train the model, a lack of transparency and consumer control over the use of their personal information for training, discrimination based

[49] *See, e.g.*, COLO. REV. STAT. §. 6-1-1309(2)(a); CONN. GEN. STAT. § 42-522(a)(3); DEL. CODE ANN. tit. 6, 12D, § 108(a)(3); IND. CODE § 24-15-6-1(b)(3); KY. REV. STAT. § 367.6(1)(c); Maryland Online Data Privacy Act of 2024, S.B. 541, 2004 Gen. Assemb., Reg. Sess. § 14-4601(A)(4); MINN. STAT. § 3250.08(b)(5); MONT. CODE § 30-14-2814(1)(c); NEB. L.B. 1074, 108th LEG. § 16(1)(c); N.H. REV. STAT. § 507-H:8(I)(c); N.J. STAT. ANN. § 56:8-166.12(c); OR. REV. STAT. § 646A.586(1)(b)(D); TENN. CODE ANN. § 47-18-3206(a)(3); TEX. BUS. & COM. CODE § 541.105(a)(3); VA. CODE § 59.1-580(A)(3). DPIA Guidelines, *supra* note 36, at Sec. III(B)(a); Republic of Croatia Personal Data Protection Agency, *List of the Types of Processing For Which a DPIA Shall Be Required Pursuant to Article 35.4 GDPR* (Dec. 13, 2018); Office of the Commissioner for Personal Data Protection, *Indicative List of Processing Operations Subject to DPIA Requirements Under Article 35(4) of GDPR*; Commission Nationale de L'informatique et des Libertés, *Deliberation N° 2018-327 of 11 Octobre 2018 on the Adoption of the List of Processing Operations for which a Data Protection Impact Assessment (DPIA) Is Required (Article 35.4 GDPR)*, (Oct. 11, 2018).

on protected classes, and reputational and psychological harm.[50] For example, researchers have been able to bypass generative models' restrictions to extract consumers' personal information as well as generate malicious code and phishing emails.[51] These models also have leaked chat prompts and certain user messages as well as payment-related information of subscribers.[52] In addition, consumers and other stakeholders have raised concerns about the use of ADMT and AI to generate deepfake imagery, which can be "overwhelmingly weaponized against women" to, for instance, create non-consensual intimate imagery.[53] In a warning to the public, the Federal Bureau of Investigation stated that it has observed an increase in the use of deepfakes to extort victims with demands of payment or to provide sexually-

---

[50] *See, e.g.*, Simon Fondrie-Teitler & Amritha Jayanti, *Consumers Are Voicing Concerns About AI*, FED. TRADE COMM'N TECH. BLOG (Oct. 3, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/10/consumers-are-voicing-concerns-about-ai; Bhaskar Chakravorti, *AI's Trust Problem*, HARVARD BUS. REV. (May 3, 2024), https://hbr.org/2024/05/ais-trust-problem; Ilkhan Ozsevim, *Consumer Concerns: AI Privacy, Transparency and Emotionality*, AI MAGAZINE (June 23, 2023), https://aimagazine.com/articles/ai-privacy-transparency-and-emotionality-consumer-concerns; *WHO Calls for Safe and Ethical AI for Health*, WORLD HEALTH ORGANIZATION [WHO] (May 16, 2023), https://www.who.int/news/item/16-05-2023-who-calls-for-safe-and-ethical-ai-for-health; Laura Weidinger et al., *Ethical and Social Risks of Harm from Language Models*, (Dec. 2021) (manuscript), https://arxiv.org/pdf/2112.04359; Rachel Goodman, *Why Amazon's Automated Hiring Tool Discriminated Against Women*, AM. C.L. UNION (Oct. 12, 2018), https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against; Pocard, *supra* note 39.

[51] Jeremy White, *How Strangers Got My Email Address From ChatGPT's Model*, N.Y. TIMES (Dec. 22, 2023), https://www.nytimes.com/interactive/2023/12/22/technology/openai-chatgpt-privacy-exploit.html; Sam Sabin, *Hackers Could Get Help from the New AI Chatbot*, AXIOS (Jan. 3, 2023), https://www.axios.com/2023/01/03/hackers-chatgpt-cybercrime-help.

[52] OpenAI, *March 20 ChatGPT Outage: Here's What Happened* (Mar. 24, 2023), https://openai.com/index/march-20-chatgpt-outage/; *see also* Tonya Riley, *AI Chatbots Want Your Geolocation Data. Privacy Experts Say Beware.*, CYBERSCOOP (June 8, 2023), https://cyberscoop.com/ai-chatbots-privacy-geolocation-data-google/.

[53] *Deepfake Explicit Images of Taylor Swift Spread on Social Media. Her Fans Are Fighting Back*, AP NEWS (Jan. 26, 2024), https://apnews.com/article/taylor-swift-ai-images-protecttaylorswift-nonconsensual-d5eb3f98084bcbb670a185f7aeec78b1; Skylar Harris & Artemis Moshtaghian, *High Schooler Calls for AI Regulations After Manipulated Pornographic Images of Her and Others Shared Online*, CNN (Nov. 4, 2023), https://www.cnn.com/2023/11/04/us/new-jersey-high-school-deepfake-porn/index.html. *See also* Nitasha Tiku & Pranshu Verma, *AI Hustlers Stole Women's Faces to Put in Ads. The Law Can't Help Them.*, WASH. POST (Mar. 28, 2024), https://www.washingtonpost.com/technology/2024/03/28/ai-women-clone-ads/; Matt O'Brien & Haleluya Hadero, *AI-generated Child Sexual Abuse Images Could Flood the Internet. Now There Are Calls for Action*, AP NEWS (Oct. 25, 2023), https://apnews.com/article/ai-artificial-intelligence-child-sexual-abuse-c8f17de56d41f05f55286eb6177138d2.

themed images or videos, and that once circulated, victims can face significant challenges in preventing the continual sharing of this content or removing it from the internet.[54] The lack of adequate recourse for victims after they suffer these privacy harms underscore the importance of conducting risk assessments to identify and mitigate risks before processing consumers' personal information to train these technologies. Lastly, this subsection also works to harmonize California law with risk factors that would require a data privacy impact assessment in the European Union.[55]

Subsection (c) provides illustrative examples of when a business must conduct a risk assessment. The examples in **subsections (c)(1)–(2)** address the use of ADMT in the ridesharing and hiring contexts, which is necessary to provide clarity about when a use of ADMT for significant decisions falls within scope of the risk-assessment requirements. Similarly, **subsection (c)(3)** addresses the disclosure of precise geolocation and other sensitive personal information to an analytics provider, which is necessary to provide clarity about when processing of sensitive personal information requires a risk assessment. **Subsection (c)(4)** provides an example of extensive profiling (specifically, profiling for behavioral advertising) and sharing of personal information, which is necessary to clarify how a processing activity can meet multiple thresholds set forth in section 7150(b) that would require a risk assessment. **Subsection (c)(5)** provides an example of Wi-Fi tracking in grocery stores, which is necessary to clarify when a business can be subject to the risk-assessment requirements for its use of ADMT for public profiling. Lastly, **subsection (c)(6)** provides an example of a business seeking to train a facial-recognition technology, which is necessary to clarify when a business would be subject to the risk-assessment requirements for training AI or ADMT that is capable of being used to establish individual identity. This subsection benefits both businesses and consumers by providing real-world examples of when businesses must conduct a risk assessment under the thresholds of subsection (b), which can be used to identify other real-world use cases that would fall within scope of section 7150(b) and require a risk assessment.

---

[54] Public Service Announcement, Alert No. I-060523-PSA, *Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes*, FBI (June 5, 2023), https://www.ic3.gov/Media/Y2023/PSA230605.

[55] *See* DPIA Guidelines, *supra* note 36, at Sec. III(B)(a).

§ 7151. Stakeholder Involvement for Risk Assessments.

The purpose of section 7151 is to provide clarity and guidance to businesses about who must be involved in conducting a risk assessment and the types of external parties that businesses may consult as part of the risk-assessment process.

Subsection (a) states that businesses must ensure that relevant individuals at the business prepare, contribute to, or review the risk assessment, based upon their involvement in the processing activity. The subsection clarifies that "relevant" individuals are those whose job duties pertain to the processing activity and provides examples of these types of individuals. Lastly, the subsection states that these individuals must make good-faith efforts to disclose all facts necessary to conduct the risk assessment and must not misrepresent any facts for the risk assessment.

The purpose of **subsection (a)** is to explain who must be involved in the risk-assessment process, which is based upon their level of involvement in the processing activity. **Subsection (a)** is necessary because a risk assessment requires that businesses identify the benefits and potential risks of a given processing activity, and this proposed subsection clarifies the steps a business must take to do so and ensures that risk assessments are conducted with full information by those involved in the processing activity. If a business did not involve all relevant individuals in the risk-assessment process, it would not be able to adequately identify benefits and risks. In addition, **subsection (a)'s** requirement that these individuals make good-faith efforts to provide all necessary facts and its prohibition against misrepresentation is necessary to ensure that businesses have all necessary and accurate information to conduct the risk assessment.

Subsection (b) states that a risk assessment may involve external parties to identify, assess, and mitigate privacy risks. The subsection also provides examples of the types of external parties that may be involved in the risk-assessment process. The purpose of this subsection is to explain that external parties can be involved in the risk-assessment process. This subsection is necessary to provide guidance to businesses on the types of external parties with which they may consult. Without this subsection, a business may be concerned it would be prohibited from consulting with external parties and lose the benefit of additional expertise in conducting its risk assessment. This subsection benefits both consumers and businesses by providing guidance on who may be involved in the

risk-assessment process to ensure that businesses can adequately identify the benefits and potential risks of a given processing activity.

§ 7152. Risk Assessment Requirements.

The purpose of section 7152 is to provide clarity and guidance to businesses regarding how to conduct a risk assessment.

Subsection (a) clarifies that the purpose of a risk assessment is to determine whether the risks to consumers' privacy outweigh the benefits for a given processing activity. It also explains how a business must conduct a risk assessment. It is necessary to implement and operationalize the statutory requirement that businesses identify the benefits and risks to consumers' privacy associated with a given processing activity.

Subsection (a)(1) requires that a business specifically identify why it will be processing consumers' personal information and prohibits identifying this purpose in generic terms. This subsection is necessary to ensure that the business identifies its purpose for processing consumers' personal information with specificity so that it can identify the benefits and potential risks of that activity.

Subsection (a)(2) requires the business to identify the categories of personal information to be processed, whether they include sensitive personal information, and, in paragraph **(A)**, the minimum personal information necessary to achieve the purpose of the processing. Paragraph **(B)** also requires a business to identify its actions to maintain data quality for certain uses of ADMT or AI. **Subsection (a)(2)(B)(i)** provides a definition of "quality of personal information," which includes completeness, representativeness, timeliness, validity, accuracy, consistency, and reliability of sources. Lastly, **subsection (a)(2)(B)(ii)** provides examples of the types of actions a business may take, such as identifying the source of the personal information and whether that source is reliable; identifying how the personal information is relevant to the task being automated and how it is expected to be useful for the development, testing, and operation of the ADMT or AI; identifying whether the personal information contains sufficient breadth to address the range of real-world inputs the ADMT or AI may encounter; and identifying how errors from data entry, machine processing, or other sources are measured and limited.

The purpose of this subsection is to ensure that businesses identify the personal information they need for the processing activity. It also implements the statutory

language that businesses identify whether the processing involves sensitive personal information. Lastly, with respect to certain uses of ADMT and AI, identifying the actions the business has taken or plans to take to maintain the quality of personal information ensures that a business can identify and address risks to consumers' privacy that result from poor data quality as part of the risk-assessment process, such as harmful bias and inaccurate decisionmaking.[56] **Subsection (a)(2)(B)(ii)'s** list of actions provides guidance to businesses to help them identify and mitigate those risks. For example, identifying whether the source of personal information is reliable and what personal information is relevant for the task being automated can assist a business in identifying and mitigating the risks of discrimination and inaccuracies in decisionmaking. This subsection is also consistent with proposed federal approaches to identifying risks associated with data quality.[57]

Subsection (a)(2) is necessary to provide clarity and guidance to businesses regarding what information is necessary to adequately identify the benefits and potential risks of a given processing activity, specifically the personal information that is necessary for the processing, whether sensitive personal information is involved, and what actions need to be taken to maintain data quality.

Each of these elements is necessary for a business to meaningfully understand and identify the benefits and potential risks of a given processing activity. The amount and nature of risk to consumers' privacy depends upon the types of personal information being processed. For example, processing a consumer's precise geolocation over time poses more risk to their privacy than processing their postal address, because precise geolocation over time enables the consistent tracking of a consumer's movements and can reveal additional sensitive personal information about them, such as frequent visits to healthcare facilities. Similarly, the risk to consumers' privacy increases with the amount of personal information being processed. For example, the retention of large amounts of personal information for a processing activity creates a larger risk to consumers' privacy if there is unauthorized access to their information. The type and amount of information

---

[56] *See* NIST AI RMF, *supra* note 2; Fair, *supra* note 46.

[57] *See* Memorandum from Shalanda D. Young, Dir. of Off. of Mgmt. and Budget, on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (2023), *available at* https://www.whitehouse.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-draft-for-public-review.pdf.

processed also affects the relevant safeguards that a business identifies as part of the risk assessment. In addition, as discussed above, issues with data quality can increase the risk of discriminatory harms and harms to consumers from inaccurate information used in decisionmaking.

Lastly, identifying the actions a business has taken or plans to take to maintain data quality is necessary to (1) ensure that the business has considered the risks to consumers' privacy that may result from poor data quality, and (2) facilitate the business's identification of the residual risks that its use of ADMT or AI poses to consumers' privacy. For example, a business that processes personal information to train ADMT but does nothing to maintain the quality of the information it is processing creates a greater risk that the ADMT's outputs will be inaccurate. Inaccurate ADMT outputs can then create additional negative impacts on consumers (for example, if that ADMT is used to make significant decisions about consumers using inaccurate data).

Subsection (a)(3) requires a business to identify the following operational elements of the process activity:

- The planned method of processing and the sources of personal information;
- The length of, and criteria for, retention;
- The relationship between the consumer and the business;
- The approximate number of consumers whose personal information the business seeks to process;
- Relevant disclosures made to the consumer, how they were made, and relevant actions to make the disclosures specific, explicit, prominent, and clear to the consumer;
- Names or categories of relevant entities in the processing activity, the purpose for disclosing personal information to them, and actions taken to make the consumer aware of these entities' involvement; and
- The technology to be used, including the logic of relevant ADMT, its output, and how the business will use that output.

Subsection (a)(3) is necessary to provide clarity and guidance to businesses about which operational elements are necessary to identify to adequately determine the benefits and potential risks of a given processing activity. These operational elements, such as the planned method of processing and the sources of personal information, affect the nature of the risk to consumers' privacy. Similarly, the relationship that a business has with consumers and the specificity, explicitness, prominence, and clarity of the business's disclosures affects whether the business's processing is consistent with consumers' reasonable expectations regarding the purposes for which their personal information will be processed. Moreover, identifying the length of retention of the personal information, the other entities involved in the processing, and the technology to be used is necessary to, for example, assess the risk of unauthorized access and to identify and implement relevant safeguards. Lastly, the approximate number of consumers whose personal information is processed also affects the magnitude of a given benefit or risk and may affect the safeguards that a business plans to implement.

Subsection (a)(4) requires a business to specifically identify the benefits to the business, the consumer, other stakeholders, and the public from the processing of the personal information. It provides an example of what would not meet the specificity requirement. Lastly, it requires that a business that profits monetarily from the activity identify this benefit and, when possible, estimate the expected profit. **Subsection (a)(4)** is necessary to implement the statutory language that businesses identify the benefits of a given processing activity when conducting a risk assessment. It also clarifies that benefits cannot be stated in a generalized manner, which is necessary to ensure that businesses can adequately identify the actual or expected benefits of a processing activity, including any expected monetary benefit.

Subsection (a)(5) requires a business to specifically identify the negative impacts to consumers' privacy associated with the processing, including the sources and causes of these negative impacts and any criteria used to make these determinations. This subsection also identifies different types of negative impacts to consumers' privacy that the business may consider. **Subsection (a)(5)** is necessary to implement the statutory language that businesses identify the potential risks to consumers' privacy of a given processing activity. Because the term "risk" without further clarification may be confusing to businesses and consumers, the regulation uses the term "negative impacts" to make the regulations easier to understand. Similarly, this subsection provides clarity and

guidance for businesses and consumers about the potential negative impacts that a business may consider. The list of negative impacts (unauthorized access, discrimination, impairment of consumer control, coercion, chilling of exploration of ideas, economic harms, physical harms, reputational harms, and psychological harms) stems from identified privacy harms in academic scholarship and other privacy frameworks.[58] This is necessary because businesses may not adequately identify the various types of privacy harms a given processing activity can cause to consumers.[59] This proposed regulation benefits both businesses and consumers by clarifying what a "risk" is in the context of consumer privacy.

Subsection (a)(6) requires a business to identify the safeguards it plans to implement to address the negative impacts it has identified, including how these safeguards address those negative impacts, and any safeguards the business will implement to maintain knowledge of emergent risks and countermeasures. This subsection is necessary because the relevant safeguards that a business plans to implement affects whether the risks to consumers' privacy outweigh the benefits of a given activity, and accordingly, whether the processing would be permitted under the CCPA. This subsection also is necessary to ensure businesses identify relevant safeguards as part of the risk-assessment process. This subsection benefits both businesses and consumers by clarifying that identification of safeguards to mitigate privacy risks to consumers are an essential part of the risk assessment.

Subsection (a)(6)(A) states the different safeguards that a business may consider. This subsection is necessary to provide guidance and clarity to businesses about the different safeguards they may consider and identify as part of the risk-assessment process. These safeguards include security controls (e.g., encryption), use of privacy-enhancing technologies, consulting external parties, and evaluating the need for human involvement as part of the business's use of ADMT and implementing policies, procedures, and training to address the degree and details of human involvement identified as necessary in that evaluation. These were selected by the Agency in its expertise on potential safeguards, and provided for

---

[58] *See, e.g.*, Danielle K. Citron & Daniel J. Solove, *Privacy Harms*, 102 BOSTON UNIV. L. REV. 793 (2022); *Resolution on Artificial Intelligence and Employment*, GLOB. PRIV. ASSEMBLY (Oct. 2023); COLO. CODE REGS. § 904-3 8.04(A)(6).

[59] *See, e.g.*, *FTC v. Rite Aid Corp.*, Case No. 2:23-cv-6023, Complaint for Permanent Injunction and Other Relief, para. 36 (Dec. 19, 2023) [hereinafter Rite Aid Complaint].

businesses' consideration as guidance on different safeguards that could be relevant for its processing activities.

Subsection (a)(6)(B) requires a business to identify, for certain uses of ADMT, whether it evaluated the ADMT to ensure it works as intended and does not discriminate based upon protected classes. It also requires the business to identify the policies, procedures, and training the business has implemented or plans to implement to ensure the ADMT works as intended and does not discriminate based upon protected classes. This subsection provides an example of how paragraphs **(B)(i)** and **(ii)** work together in the context of evaluating a facial-recognition technology. Subsection **(B)(iii)** clarifies that when a business has obtained the ADMT from another person, it must identify whether it reviewed that person's evaluation of the ADMT, including any requirements or limitations relevant to the business's proposed use as well as any accuracy and nondiscrimination safeguards the business implemented or plans to implement. This subsection is necessary because whether a business has evaluated its use of ADMT and implemented accuracy and nondiscrimination safeguards affects whether the risks to consumers' privacy outweigh the benefits of a given activity, and accordingly, whether the processing would be permitted under the CCPA.[60] The example provided in the subsection illustrates how the evaluation and implementation of safeguards would affect the risk assessment: a facial-recognition technology without appropriate accuracy safeguards poses a higher risk to consumers' privacy than one deployed with appropriate safeguards.[61]

Lastly, this subsection is necessary to operationalize this requirement for businesses that have not developed an ADMT themselves, but rather are using an ADMT that they have obtained from another person. These businesses would only have to identify whether they reviewed that person's evaluation of the ADMT and any relevant accuracy and nondiscrimination safeguards they implemented or plan to implement, which also benefits these businesses by lessening their burden of compliance.

Subsection (a)(7) requires a business to identify whether it will initiate the processing activity. This subsection is necessary to ensure that a business identifies

---

[60] *See* NIST AI RMF, *supra* note 2.

[61] *See, e.g.*, Rite Aid Complaint, *supra* note 59.

the conclusion of its risk-assessment process (i.e., whether it will initiate the processing), assuming that the risks to consumers' privacy do not outweigh the benefits of that activity. In addition, certain risk-assessment requirements apply only if the business initiated the processing. For example, a business is not required to submit an abridged risk assessment to the Agency if it did not initiate the processing under subsection 7157(b)(4)(1). Identifying whether the business initiated the processing is necessary to determine whether the business must comply with these additional requirements. This subsection also benefits businesses by ensuring they maintain proper records of whether they initiated the processing, particularly as they comply with other risk-assessment requirements regarding updating risk assessments and submitting risk-assessment materials to the Agency.

Subsection (a)(8) requires businesses to identify who contributed to the risk assessment. Businesses have the option to either do so in the risk assessment itself, or in a separate document. This subsection is necessary to ensure that businesses maintain a record of who contributed to the risk assessment, so that the information reflected in the risk assessment can be traced to relevant actors internal or external to the business. This also benefits businesses, so that when they must update their risk assessments, they can easily identify relevant contributors to ensure the consistency and accuracy of their risk assessments over time.

Subsection (a)(9) requires businesses to identify when the risk assessment was reviewed and approved, and by whom. In addition, the subsection states that the individuals who review and approve the risk assessment must include the individual who decides whether the business will initiate the processing activity. Lastly, the subsection requires that if a business presents the risk assessment for review to its board of directors, governing body, or highest-ranking executive responsible for oversight of risk-assessment compliance, then the business include the date of that review as well.

The purpose of this subsection is to ensure that businesses maintain accurate records of when they reviewed and approved their risk assessments and who at the business was responsible for that review and approval. This subsection is necessary to ensure accountability during the risk-assessment process through documentation of when that assessment was conducted and who decided to approve it. This addresses feedback received during the preliminary comment

period that risk assessments can be merely documentation exercises rather than practical tools to identify and manage risk. Internal accountability, such as through the documentation of dates and reviewers/approvers, is necessary so that businesses do not treat risk assessments as paperwork, but rather as meaningful exercises to identify and address risks to consumers' privacy. This subsection also benefits businesses by ensuring they keep accurate records of their risk assessment, which eases their compliance with other risk-assessment requirements. For example, by documenting when the risk assessment was conducted, the business can easily identify when three years has passed so it can conduct a review for accuracy in compliance with section 7155(a)(2). In addition, by documenting who reviewed and approved the risk assessment, the business can also easily identify which individuals should be contacted when reviewing and updating, as needed, the risk assessment.

Section 7152's requirements work to harmonize the application of California law with the requirements and guidelines in other U.S. states and in the European Union.[62] This subsection benefits businesses by providing a structured method by which they can identify the risks and relevant safeguards for their processing activities.[63] In addition, risk assessments are cost effective for businesses, because they enable issues to be identified before the processing begins, which means changes are simpler and less costly relative to later stages of the processing.[64] This section also benefits consumers by ensuring they are not subject to unnecessary and unmitigated risk when a business wants to engage in any of the activities set forth in section 7150.

§ 7153. Additional Requirements for Businesses that Process Personal Information to Train Automated Decisionmaking Technology or Artificial Intelligence.

The purpose of section 7153 is to provide clarity and guidance about the disclosures a business must make if it is processing personal information to train ADMT or AI. This section is necessary to ensure that recipients of these

---

[62] *See, e.g.*, 4 COLO. CODE REGS. § 904-3-8.04; Colorado Artificial Intelligence Act, S.B. 24-205, 74th Gen. Assemb., Reg. Sess. (CO. 2024); DPIA Guidelines, *supra* note 36, at Sec. III(B)(c).

[63] *See* Felix Bieker et al., *Data Protection Impact Assessment: A Hands-On Tour of the GDPR's Most Practical Tool*, PRIV. AND IDENTITY MGMT, SPRINGER INT'L PUBL'G, pp. 207-220 (2018).

[64] *See* Leonardo Horn Iwaya et al., Privacy Impact Assessments in the Wild: A Scoping Review (2024).

technologies have all the required information (e.g., the requirements and limitations relevant to the permitted uses of the technology) to use them without unnecessary and unmitigated risk to consumers' privacy. This section benefits businesses by ensuring they have all necessary information to conduct risk assessments and benefits consumers by ensuring that other persons who receive and use these technologies are aware of any requirements or limitations of use. It also works to harmonize the application of California law with requirements in the Colorado Artificial Intelligence Act and guidelines proposed by the NIST.[65]

For businesses that make ADMT or AI available to other businesses for any of the activities set forth in section 7152, **subsection (a)** requires them to provide all necessary facts to those recipient-businesses to conduct their own risk assessments. This subsection is necessary to address circumstances where a business is deploying ADMT or AI for processing that presents significant risk to consumers' privacy but did not develop that ADMT or AI itself, so that the business has all relevant facts to properly identify benefits, potential risks, and safeguards.

For businesses that train ADMT or AI as set forth in section 7150(b)(4) and permit other persons to use that technology, **subsection (b)** requires them to provide a plain language explanation of any relevant requirements or limitations associated with the permitted uses of that technology. The purpose of this subsection is to ensure that businesses that train such ADMT or AI notify downstream users of requirements or limitations that could increase the risk to consumers' privacy if not disclosed. This subsection is necessary to address risks to consumers' privacy that could occur if such technologies were provided to persons who may not be aware of requirements or limitations on use.

Subsection (c) states that the requirements in subsections (a) and (b) only apply to ADMT or AI trained using personal information. This subsection is necessary to clarify that ADMT or AI that was not trained on personal information is exempt from this regulation. The risk-assessment regulations focus on the processing of consumers' personal information that presents significant risk to consumers' privacy. Accordingly, these regulations are intended to address ADMT or AI that process consumers' personal information.

---

[65] *See, e.g.*, Colorado Artificial Intelligence Act, S.B. 24-205, 74th Gen. Assemb., Reg. Sess. (CO. 2024); NIST AI RMF, *supra* note 2.

§ 7154. Prohibition Against Processing If Risks to Consumers' Privacy Outweigh Benefits.

The purpose of section 7154 is to provide clarity and guidance to businesses about the goal of a risk assessment.

Subsection (a) states that businesses must not process personal information for any processing activity set forth in subsection 7150(b) if the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public from the processing. The purpose of this subsection is to prohibit processing where risks outweigh the benefits. This subsection is necessary to implement and operationalize the statutory direction that the goal of a risk assessment is to restrict or prohibit processing activities where the risks to consumers' privacy outweigh the benefits of those activities. It 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.

§ 7155. Timing and Retention Requirements for Risk Assessments.

The purpose of section 7155 is to provide clarity and guidance to businesses regarding when they must conduct, review, and update their risk assessments and for how long they must retain these risk assessments. This section is necessary to clarify the timing requirements for businesses, so that they conduct and update risk assessments in a manner that protects consumers' privacy. It also is necessary to clarify the retention requirements for these risk assessments, so that the Agency and Attorney General can review them to ensure compliance with the CCPA.

Subsection (a) addresses the timing requirements for risk assessments.

Subsection (a)(1) requires businesses to conduct and document their risk assessments before initiating any of the activities identified in section 7150(b). This subsection is necessary to clarify that a risk assessment must be conducted and documented before initiating the activity. A risk assessment must be conducted before a processing activity is initiated because otherwise the processing activity could have negative impacts on consumers' privacy that a business would not identify and mitigate until after it started the activity. This section benefits both businesses and consumers by clarifying when a risk assessment must be conducted during the lifecycle of a processing activity and ensuring that businesses identify

negative impacts and implement appropriate safeguards prior to the start of an activity.

Subsection (a)(2) requires businesses to review their risk assessments at least once every three years for accuracy and update them as needed. This subsection is necessary to clarify that risk assessments address risks to consumers' privacy throughout a processing activity's lifecycle, and not simply at the start of that activity. This subsection also is necessary to ensure that risk assessments do not reflect out-of-date information, to the extent that there are changes to processing activities. This approach is consistent with the approaches taken under the Colorado Privacy Act and the European Union's GDPR, which require or provide guidance to periodically review risk assessments.[66] This subsection benefits businesses and consumers by ensuring that businesses continue to ensure that risks to consumers' privacy are accurately identified and mitigated when engaging in an activity that poses significant risks to consumers' privacy.

Subsection (a)(3) requires businesses to immediately update their risk assessments whenever there is a material change to the processing activity. The subsection defines a "material" change to clarify when this requirement applies. Specifically, a change is material when it diminishes the benefits of the activity, creates new negative impacts or increases their likelihood or magnitude, or diminishes the effectiveness of safeguards. Lastly, the subsection provides several examples of material changes as guidance for businesses regarding the types of changes that could fall within the scope of this requirement. These examples include changes to the purpose of the processing; the minimum personal information necessary for the processing; or risks to consumers' privacy raised by consumers. Changes to the purpose of the processing and the personal information used for the processing can create new risks to consumers' privacy, such as impairing their control over their personal information. In addition, if consumers are raising concerns about privacy risks of a given activity, this can serve as a helpful indicator to a business that the magnitude or likelihood of a previously identified negative impact has increased, or that there is a new negative impact associated with the processing activity that the business has not previously identified.

---

[66] *See* 4 COLO. CODE REGS. § 904-3-8.05(C) (requiring annual review and updates to certain risk assessments); DPIA Guidelines, *supra* note 36, at Sec. III(B)(c) (providing guidance that risk assessments should be re-assessed after three years, or sooner).

This subsection is necessary because material changes in a processing activity can affect whether the risks to consumers' privacy outweigh the benefits associated with the activity, and therefore whether the processing is prohibited under section 7154. In addition, this subsection is necessary to prevent unidentified or increased negative impacts that could otherwise occur due to material changes in processing activities. This approach is consistent with approaches taken in the Colorado Privacy Act and the European Union's GDPR, which require or provide guidance to update risk assessments whenever there is a material change in the processing activity.[67] The subsection benefits both businesses and consumers by ensuring that even when there are material changes to a processing activity, a business continues to identify and mitigate risks to consumers' privacy.

Subsection (b) requires businesses to retain their risk assessments for as long as the activity continues, or for five years after completion of the risk assessment, whichever is later. This subsection is necessary to specify the duration that businesses must retain risk assessments to demonstrate compliance with the CCPA. It addresses the need to maintain records to prove compliance, and it assists in the enforcement of the law if the unabridged risk assessment is requested by the Agency or Attorney General. It also is consistent with the time period during which the Agency may bring an administrative action alleging a violation of the CCPA. (*See* Civ. Code, § 1798.199.70.)

Subsection (c) requires that a business conduct a risk assessment for any processing activity set forth in section 7150(b) that is ongoing after the effective date of these regulations. The proposed subsection allows businesses to do so within 24 months of the effective date of these regulations. This subsection is necessary to clarify businesses' requirements for activities that pose significant risk to consumers' privacy that were initiated before the effective date of these regulations but that continue after that date. The requirement to conduct a risk assessment within 24 months balances the need to ensure that businesses identify and mitigate risks for these activities while giving those businesses sufficient time to work through potential backlogs of processing activities. This subsection benefits businesses by clarifying their responsibilities for all of their processing activities subject to section 7150(b), and benefits consumers by ensuring their

[67] *See* 4 COLO. CODE REGS. § 904-3-8.05(D); DPIA Guidelines, *supra* note 36, at Sec. III(B)(c).

privacy is protected if a business is engaging in any of those activities after the effective date of these regulations.

§ 7156. Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations.

The purpose of section 7156 is to explain when a business may use a single risk assessment for multiple processing activities or to comply with the CCPA's requirements when those requirements overlap with risk-assessment requirements under other laws. This section is necessary to clarify that a business does not need to duplicate its work across multiple risk assessments. This section benefits businesses by providing them flexibility to use a single risk assessment for multiple activities or to comply with the CCPA and other laws, while ensuring that the CCPA's requirements are satisfied.

Subsection (a) explains that a business may conduct a single risk assessment for a comparable set of processing activities. It defines "comparable set of processing activities" as a set of similar processing activities that present similar risks to consumers' privacy and provides an example of when a single risk assessment can address these activities. The example illustrates that a single risk assessment can be used when in each case the business is collecting the same personal information in the same way for the purpose of sending coupons and age-appropriate toy lists to children, and this processing presents similar risks to consumers' privacy.

This subsection is necessary to clarify when businesses can use a single risk assessment for multiple processing activities. This subsection benefits businesses by providing a standard for them to use to identify when they can consolidate activities into a single risk assessment. This approach also works to harmonize application of California law with similar guidance for businesses in twelve other U.S. states and in the European Union.[68]

Subsection (b) explains that businesses that conduct and document a risk assessment to comply with another law or regulation are not required to conduct a

---

[68] *See, e.g.,* 4 COLO. CODE REGS. § 904-3-8.02(D); IND. CODE § 24-15-6-1(d); Maryland Online Data Privacy Act of 2024, S.B. 541, 2004 Gen. Assemb., Reg. Sess. § 14-4601(E); MINN. STAT. § 3250.08(h); MONT. CODE § 30-14-2814(4); NEB. L.B. 1074, 108th LEG. § 16(5); N.H. REV. STAT. § 507-H:8(IV); N.J. STAT. ANN. § 56:8-166.12(d); OR. REV. STAT. § 646A.586(1)(c); TENN. CODE ANN. § 47-18-3206(d); TENN. CODE ANN. § 47-18-3206(d); VA. CODE § 59.1-580(D). *See also* DPIA Guidelines, *supra* note 36, at Sec. III(A).

duplicative risk assessment for the CCPA. This subsection also states that if that risk assessment does not meet all of the risk-assessment requirements of the CCPA, then a business must supplement the risk assessment with any required information to meet all of the requirements of these regulations. This subsection is necessary to clarify that business can use a single risk assessment for the same activity conducted across multiple jurisdictions that have risk-assessment requirements. It also is necessary to clarify that if other jurisdictions' laws do not have all of the requirements of these regulations, then a business must address the CCPA's additional requirements. This is necessary to prevent businesses from trying to use a risk assessment that does not include all the CCPA's required information to comply with this Article, or from seeking to only comply with the risk-assessment requirements of other jurisdictions that impose requirements that are not as thorough and privacy-protective as those in these regulations. This subsection benefits businesses by providing them with flexibility and reducing their burden when operating in multiple jurisdictions, while ensuring that risk assessments consistently meet the requirements set forth in Article 10.

§ 7157. Submission of Risk Assessments to the Agency.

The purpose of section 7157 is to provide clarity and guidance to businesses about what must be submitted to the Agency and the timing of that submission. This section is necessary to implement and operationalize the statutory direction that risk assessments be submitted to the Agency on a regular basis.

Subsection (a) addresses when businesses must submit risk-assessment materials to the Agency. **Subsection (a)(1)** states that businesses must submit their first risk-assessment materials to the Agency within 24 months of the effective date of these regulations. **Subsection (a)(2)** states that after the first submission, subsequent risk-assessment materials must be submitted every calendar year. **Subsection (a)(2)** also states that there cannot be a gap in the months covered by successive submissions.

Because the CCPA states that risk assessments will be submitted on a regular basis to the Agency, this subsection is necessary to clarify that "a regular basis" is every calendar year. An annual submission ensures continual compliance with the risk-assessment regulations and promotes consistency across the risk-assessment and cybersecurity-audit regulations, the latter of which similarly requires completion on an annual basis. This subsection also is necessary to clarify that

businesses have 24 months from the effective date of these regulations for their first submission, which gives businesses additional time to set up their risk-assessment processes before their first submission. This subsection benefits businesses by providing a clear timeline for when businesses must submit their materials to the Agency and lessening their burden of compliance prior to the first submission.

Subsection (b) addresses what risk assessment materials must be submitted to the Agency. It is necessary to clarify what must be submitted to the Agency every calendar year. It benefits both businesses and consumers by balancing the need for transparency and accountability in risk-assessment submissions with the concerns raised in preliminary rulemaking comments that businesses should not be required divulge confidential information in their annual submissions to the Agency.

Subsection (b)(1) requires businesses to submit a written certification that they have conducted their risk assessments as set forth in this Article. It also requires a business to designate the highest-ranking executive that is responsible for oversight of the business's risk-assessment compliance to certify on the business's behalf (i.e., a "designated executive"). Lastly, this subsection provides requirements for what must be included in the written certification: (1) which months the business is certifying compliance for, and the number of risk assessments that were conducted and documented during that time; (2) an attestation that the designated executive has reviewed, understood, and approved the risk assessments; (3) an attestation that the business only initiated any of the activities set forth in subsection 7150(b) after conducting and documenting a risk assessment; and (4) the designated executive's name, title, signature, and date of certification. The submission of this information in a certification is necessary to ensure accountability, so that even if the business is not submitting its unabridged risk assessments to the Agency every calendar year, the business is certifying that it has only initiated any processing set forth in subsection 7150(b) after conducting and documenting a risk assessment as set forth in this Article. The requirement that a designated executive sign this certification is also necessary to ensure accountability at the highest levels of the business when conducting, documenting, and submitting risk-assessment materials to the Agency.

Subsection (b)(2) requires businesses to submit an abridged form of their new or updated risk assessments to the Agency in their annual submissions. This subsection identifies what must be included in the abridged form of the risk

assessment: (1) identification of which activity in subsection 7150(b) triggered the risk assessment; (2) a plain language explanation of the purpose for processing consumers' personal information; (3) the categories of personal information processed, and whether they include sensitive personal information; and (4) a plain language explanation of the safeguards that the business has implemented or plans to implement for that activity, with an exception so that a business is not required provide information that would compromise security, fraud prevention, or safety. The submission of this information in abridged form is necessary to provide transparency about businesses' risk assessments without requiring public disclosure of businesses' confidential information or processes in its annual submission, which are subject to public disclosure under the Public Records Act.

Subsection (b)(3) provides businesses the option to include in their submission to the Agency a hyperlink to a public webpage that contains its unabridged risk assessment. This is necessary to provide clarity and guidance to businesses that they may provide the Agency with access to their unabridged risk assessments in their submissions.

Subsection (b)(4) provides two exemptions for businesses. First, a business is not required to submit a risk assessment if it does not initiate the processing activity subject to that risk assessment. Second, if there are no material changes to a previously submitted abridged risk assessment, the business is not required to submit an updated risk assessment in abridged form to the Agency. For the latter exception, the business would still need to submit a certification of conduct to the Agency. This is necessary to clarify when businesses are not required to submit abridged risk assessments. This subsection is also necessary to ensure that businesses meaningfully identify benefits and risks of a processing activity, without being concerned about having to submit these assessments to the Agency when they do not initiate a processing activity because the risks to consumers' privacy outweigh the benefits of that activity. In addition, the clarification that businesses do not have to submit updated risk assessments in abridged form when there are no material changes to the processing activity is necessary to simplify submission requirements for businesses and limit their burden during submission.

Subsection (c) addresses how risk-assessment materials must be submitted to the Agency. It states that they must be submitted through the Agency's website at https://cppa.ca.gov/. This subsection is necessary to clarify how these materials must be submitted.

Subsection (d) addresses when unabridged risk assessments must be submitted. It states that the Agency or the Attorney General may require a business to provide its unabridged risk assessments at any time, and that these unabridged risk assessments must be provided within 10 business days of a request from the Agency or the Attorney General. This subsection is necessary to clarify that businesses must still provide their unabridged risk assessments if requested by the Agency or Attorney General, even if those are not required to be provided in annual submissions to the Agency. This subsection also is necessary because the Agency or Attorney General may need access to the risk assessment in unabridged form to ensure compliance with the CCPA's requirements. This requirement also harmonizes the CCPA's risk-assessment requirements with those in fifteen other U.S. states, which similarly require submission of risk assessments upon request.[69]

ARTICLE 11. AUTOMATED DECISIONMAKING TECHNOLOGY

Civil Code section 1798.185, subdivision (a)(16), requires the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. The statute also directs the Agency to require businesses to provide meaningful information about the logic involved in, and to describe the likely outcome of, the decisionmaking process with respect to the consumer. The purpose of proposed Article 11 is to operationalize the requirements introduced by the CCPA, and to provide clarity and specificity to implement the law. The proposed regulations benefit businesses by providing guidance about how to respond to consumer requests to exercise their access and opt-out rights, and they benefit consumers by providing meaningful control and information with respect to businesses' use of ADMT. This proposed article is informed by public comments received by the Agency during preliminary rulemaking activities, approaches to providing meaningful control and information to consumers in academic scholarship and other frameworks, and the purpose and intent set forth in the CCPA.

---

[69] *See, e.g.*, COLO. REV. STAT. § 6-1-1309(4); CONN. GEN. STAT. § 42-522(c); DEL. CODE ANN. tit. 6, 12D, § 108(c); IND. CODE § 24-15-6-2(a); KY. REV. STAT. § 367.6(3); Maryland Online Data Privacy Act of 2024, S.B. 541, 2004 Gen. Assemb., Reg. Sess. § 14-4610(D); MINN. STAT. § 3250.08(f); MONT. CODE § 30-14-2814(3); NEB. L.B. 1074, 108th LEG. § 16(3); N.H. REV. STAT. § 507-H:8(III); N.J. STAT. ANN. § 56:8-166.12(b); OR. REV. STAT. § 646A.586(3); TENN. CODE ANN. § 47-18-3206(c); TEX. BUS. & COM. CODE § 541.105(c); VA. CODE § 59.1-580(C).

§ 7200. When a Business's Use of Automated Decisionmaking Technology is Subject to the Requirements of This Title.

Subsection (a) requires businesses to comply with Article 11's ADMT requirements when they use ADMT for: (1) a significant decision concerning a consumer; (2) extensive profiling of a consumer; or (3) training uses of ADMT.

Subsections (a)(1)–(3) respectively define what "significant decision," "extensive profiling," and "training uses of [ADMT]" mean. **Subsection (a)(1)** defines "significant decision" to mean 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, employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services. It explains that "significant decisions" include only decisions using information that is not subject to relevant data-level exceptions in the CCPA. It also identifies for businesses and consumers the types of employment or independent contracting opportunities and education and employment opportunities that are in scope of the regulation. **Subsection (a)(2)** defines "extensive profiling" to address the profiling of consumers in work and educational contexts, in publicly accessible places, and for behavioral advertising. Lastly, **subsection (a)(3)** explains that "training uses of ADMT" means processing consumers' personal information to train ADMT that is capable of being used for significant decisions, establishing individual identity, physical or biological identification or profiling, or generating deepfakes.

Subsection (a) is necessary to operationalize Civil Code section 1798.185, subdivision (a)(16), which directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT. This subsection identifies when the use of ADMT presents significant risk to consumers' privacy, and thus, warrants a consumer's ability to access and opt-out of that use of ADMT. The ADMT uses identified are informed by public comments and reports of the privacy harms posed by these uses of ADMT, including lack of consumer control over their personal information, discrimination on the basis of protected classes, and psychological and reputational harms.[70] For further discussion of the privacy

[70] *See supra* notes 43–48; *see also* Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

risks to consumers arising from these uses of ADMT, please see the discussion of subsections 7150(b)(3)–(4) above. These regulations are also informed by others' approaches to ensuring that ADMT is deployed in ways that protect consumers' privacy. This includes federal frameworks, laws, and regulations;[71] state and local

[71] *See, e.g.,* NIST AI RMF, *supra* note 2; BLUEPRINT FOR AN AI BILL OF RIGHTS, *supra* note 3; NAT'L INST. OF STANDARDS & TECH., NISTIR 8312, FOUR PRINCIPLES OF EXPLAINABLE ARTIFICIAL INTELLIGENCE (Sept. 2021), https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8312.pdf; Press Release, White House, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/; Andrew Smith, *Using Artificial Intelligence and Algorithms*, FED. TRADE COMM'N (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-algorithms; Rohit Chopra, Kristen Clarke, Charlotte A. Burrows, & Lina M. Khan, Joint Statement from the Bureau of Consumer Financial Protection, DOJ Civil Rights Division, U.S. Equal Employment Opportunity Commission, and FTC on Enforcement Efforts Against Discrimination and Bias in Automated Systems (Apr. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf; *CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms*, CONSUMER FIN. PROT. BUREAU: NEWSROOM (May 26, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/; CONSUMER FIN. PROT. BUREAU, CIRCULAR 2022-03: ADVERSE ACTION NOTIFICATION REQUIREMENTS IN CONNECTION WITH CREDIT DECISIONS BASED ON COMPLEX ALGORITHMS (May 26, 2022), https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/; EEOC, *Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964* (May 18, 2023), https://www.eeoc.gov/laws/guidance/select-issues-assessing-adverse-impact-software-algorithms-and-artificial?utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term=; Press Release, Dep't of Justice, Justice Department Files Statement of Interest in Fair Housing Act Case Alleging Unlawful Algorithm-Based Tenant Screening Practices (Jan. 9, 2023), https://www.justice.gov/opa/pr/justice-department-files-statement-interest-fair-housing-act-case-alleging-unlawful-algorithm.

laws and regulations;[72] international frameworks, laws, and guidance;[73] and academic scholarship.[74] These regulations harmonize with these other approaches, including by emphasizing the importance of transparency, risk identification and mitigation, the ability to opt-out from automated systems, explainability, avoiding harmful bias and discrimination, empirical soundness, and accountability.

---

[72] *See, e.g.*, COLO. REV. STAT. § 6-1-1306(a)(I)(C); 4 COLO. CODE REGS. §§ 904-3-6.03(A)(1)(c), 9.03, 9.04, 9.05(C); CONN. GEN. STAT. §§ 42-518(a)(1), (4), (5)(C), 42-520(c); DEL. CODE ANN. tit. 6, 12D, §§ 104(a)(1), (a)(1)(4), (a)(6)(c),106(c); IND. CODE §§ 24-15-6-1(b)(1), (b)(4)(B), (b)(5)(C); KY. REV. STAT. §§ 367.6(2)(a), (d), (e), 4(3); Maryland Online Data Privacy Act of 2024, S.B. 541, 2004 Gen. Assemb., Reg. Sess. §§ 14-4605(B)(7)(A)(4), 4607(D), (E)(1); MINN. STAT. §§ 3250.08(b)(1)-(2), (b)(4); MONT. CODE §§ 30-14-2808 (1)(a), (1)(d), (e)(iii), 2812(5); NEB. L.B. 1074, 108th LEG. § 16(1)(e)(iii); N.H. REV. STAT. §§ 507-H:4(I)(a), (d), (e), 6(III); N.J. STAT. ANN. § 56:8-166.6(a)-(b), 166.10(a)(5)(c),166.11(a)-(b); OR. REV. STAT. §§ 646A.574 (1)(a)(C), (d), 578(4); TENN. CODE ANN. §§ 47-18-3203(a)(2)(A), (D), 3204(c); TEX. BUS. & COM. CODE §§ 541.102(b)(5)(C), 541.102; VA. CODE §§ 59.1-577(A)(1), 59.1-577(A)(4), (5), 578(C). *See also* Press Release, Cal. Civil Rights Dep't, Civil Rights Council Releases Proposed Regulations to Protect Against Employment Discrimination in Automated Decision-Making Systems (May 17, 2024), https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2024/05/2024.05.17-Automated-Decisions-Regs-Release.pdf; Colorado Act Concerning Consumer Protections in Interactions with Artificial Intelligence Systems (2024) ("Colorado AI Act"); COLO. REV. STAT. § 10-3-1104.9; Attorneys General of Colorado, Connecticut, Tennessee, & Virginia et al., *Comment on Artificial Intelligence ("AI") System Accountability Measures and Policies* — Docket Number NTIA–2023–0005, 88 FR 22433 (June 12, 2023), https://oag.ca.gov/system/files/attachments/press-docs/NTIA%20AI%20Comment.pdf; Press Release, Mass. Off. of the Att'y Gen., AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities (Apr. 4, 2017); NEW YORK NY., LOCAL LAW 144 (2021); NEW YORK, NY., THE RULES OF THE CITY OF NEW YORK, Subchapter T §§ 5-300–5-304.

[73] *See* Global Privacy Assembly, *supra* note 58; OECD, Recommendation of the Council on Artificial Intelligence, § 1.3.iv, OECD Legal Instruments (May 21, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (hereinafter OECD Principle 1.3); *see also* GDPR, Articles 15(1), 21–22 (2018); Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, pp. 16-17, 25 n.40, 26 (last revised & adopted Feb. 6, 2018), http://ec.europa.eu/newsroom/document.cfm?doc_id=47711; Data Protection Act of 2018; *Accountability Framework*, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/; *Rights related to Automated Decision Making including Profiling*, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/; EU AI Act, *supra* note 2; Office of the Information & Privacy Commissioner for British Columbia, *supra* note 46.

[74] *See, e.g.*, Richardson, *supra* note 3; Margot E. Kaminski, *Understanding Transparency in Algorithmic Accountability*, in The Cambridge Handbook of the Law of Algorithms 121, 128–29 (Woodrow Barfield ed., 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3622657; Slaughter, *supra* note 43; Bernhardt et al., *supra* note 43; Vitak & Zimmer, *supra* note 43.

Similarly, the proposed transparency and opt-out requirements for training uses of ADMT are consistent with approaches taken by other agencies and data protection authorities to limit such training when it undermines consumers' control of their personal information.[75]

This subsection is also necessary to further the intent and purpose of the CCPA to strengthen consumer privacy while giving attention to the impact on business and innovation. (*See* Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3.) Specifically, this subsection ensures that consumers have meaningful information and control with respect to businesses' uses of ADMT with respect to them and creates important performance standards that support businesses' uses of these technologies in a privacy-protective manner.

Lastly, **subsections (a)(1)–(3)** are necessary to clarify what each term ("significant decision," "extensive profiling," and "training uses of ADMT") means. This ensures that businesses and consumers are aware of the uses of ADMT that are subject to the requirements set forth in this Article. For further discussion of these uses of ADMT, please see the discussion of subsections 7150(b)(3)(A), (b)(3)(B), and (b)(4) above.

§ 7201. Requirement for Physical or Biological Identification or Profiling.

The purpose of section 7201 is to provide clarity and guidance to businesses regarding when they must comply with additional requirements to ensure that the identification and profiling they use work as intended for their proposed use and do not discriminate against consumers upon the basis of protected classes.

---

[75] *See* FED. TRADE COMM'N, *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests* (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever FED. TRADE COMM'N, *California Company Settles FTC Allegations It Deceived Consumers about Use of Facial Recognition in Photo Storage App* (Jan. 11, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo; Supantha Mukherjee & Giselda Vagnoni, *Italy Restores ChatGPT After OpenAI Responds to Regulator*, REUTERS (Apr. 28, 2023); PIPEDA Findings #2021-001, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta* (Feb. 2, 2021).

Subsection (a) requires a business that uses physical or biological identification or profiling for a significant decision concerning a consumer, or for extensive profiling of a consumer, to comply with subsections (a)(1) and (a)(2). This subsection is necessary to address the privacy harms to consumers from ineffective and inaccurate identification and profiling, including discrimination upon the basis of protected classes.[76] In addition, other agencies and data protection authorities, academic scholars, and government-sponsored research have raised concerns about the efficacy and fairness of these technologies, including facial-, emotion-, and voice-recognition technologies, particularly when they are deployed in certain contexts (such as to analyze performance at work) or without appropriate safeguards at deployment.[77] Lastly, this subsection furthers the intent and purpose of the CCPA to strengthen consumer privacy while giving attention to the impact on business and innovation. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3.) It benefits businesses by providing flexible guidance as to how to evaluate these technologies and implement safeguards to ensure their efficacy, and it benefits consumers by prohibiting discrimination based upon protected classes.

Subsection (a)(1) requires such a business to either conduct an evaluation of the physical or biological identification or profiling to ensure that it works as intended for the business's proposed use and does not discriminate based upon protected classes. This requirement is necessary to place responsibility on the business using

---

[76] *See, e.g.*, Elisa Harlan & Oliver Schnuk, *Objective or Biased: On the Questionable Use of Artificial Intelligence for Job Applications*, BR24 (Feb. 16, 2021), https://interaktiv.br.de/ki-bewerbung/en/; Alex Engler, *For Some Employment Algorithms, Disability Discrimination by Default*, BROOKINGS INST. (Oct. 31, 2019), https://www.brookings.edu/articles/for-some-employment-algorithms-disability-discrimination-by-default/.

[77] *See, e.g.*, Global Privacy Assembly, *supra* note 58; Rite Aid Complaint, *supra* note 59; Fair, *supra* note 46; EEOC Job Applicant and Employee Guidance, *supra* note 3; EEOC, Transcript of the meeting of January 31, 2023 - Navigating Employment Discrimination in AI and Automated Systems: A New Civil Rights Frontier (Jan. 31, 2023), https://www.eeoc.gov/meetings/meeting-january-31-2023-navigating-employment-discrimination-ai-and-automated-systems-new/transcript; Citron & Solove, *supra* note 58; Slaughter, *supra* note 43; Keith E. Sonderling et al., *The Promise and The Peril: Artificial Intelligence and Employment Discrimination*, 77 U. MIAMI LAW. REV. 1(3) (2022), https://repository.law.miami.edu/umlr/vol77/iss1/3; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. OF MACH. LEARNING RSCH. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; *The National Academies Press*, NAT'L ACADS. OF SCI., ENGINEERING & MEDICINE, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Washington, DC: The National Academies Press (2024), https://nap.nationalacademies.org/login.php?record_id=27397.

the identification or profiling to ensure that it is working properly and not discriminating against consumers. However, the subsection affords businesses flexibility as to how to conduct their evaluation. For example, if the business obtained the technology from another person, the business must review that person's evaluation, including any relevant requirements or limitations, but the business is not required to conduct its own evaluation of the technology (see **subsection (a)(1)(A)**). Together with subsection 7153(b)—which requires a business that trains ADMT to provide a plain language explanation of any requirements or limitations of the technology to the persons who use it—this subsection ensures that the business using the technology has the information it needs to review the technology to ensure it works for its intended use (e.g., taking into account its industry, as well as the populations, locations, and contexts in which it will deploy the technology).

Subsection (a)(2) requires such a business to implement policies, procedures, and training to ensure that the physical or biological identification or profiling works as intended for the business's proposed use and does not discriminate based upon protected classes. This subsection is necessary because if these technologies are deployed without sufficient safeguards, they can cause privacy harm to consumers that cannot be reasonably avoided.[78]

Subsections (a)(1) and **(a)(2)** together provide flexible, performance-based requirements for businesses, by requiring them to take steps to ensure that their use of physical or biological identification or profiling will be work as intended for their proposed use and will avoid discrimination upon the basis of protected classes. As noted above, these subsections are necessary to provide clarity and guidance to businesses and to ensure that businesses do not deploy identification or profiling technologies in ways that cause significant privacy harm to consumers.

§ 7220. Pre-use Notice Requirements.

The purpose of section 7220 is to ensure that consumers whose personal information will be processed by a business using ADMT in the ways set forth in subsection 7200(a) have meaningful information and an opportunity to exercise their rights to opt-out of or access ADMT.

---

[78] *See, e.g.*, Rite Aid Complaint, *supra* note 59.

Subsection (a) clarifies that a business using ADMT as set forth in subsection 7200(a) must provide a Pre-use Notice to consumers that informs consumers about the business's use of ADMT and the consumers' rights to opt-out of, and to access information about, the business's use of ADMT. This subsection is necessary because consumers can only meaningfully exercise their rights if they know their personal information is about to be processed and how the technology would work (i.e., a Pre-use Notice is a prerequisite for exercising their rights). A Pre-use Notice is necessary and critical to implementing consumers' opt-out and access rights. Without a Pre-use Notice consumers would not be given a meaningful opportunity to opt-out prior to the use of the ADMT with respect to them, nor would they have sufficient information about how the ADMT works to decide whether to exercise their opt-out and access rights.

Subsection (b) provides clear guidance for businesses about how a Pre-use Notice must be provided. Specifically, **subsection (b)(1)** requires that the Pre-use Notice comply with subsections 7003(a)–(b), which set forth requirements for disclosures and communications to consumers to ensure they are: easy-to-read and understandable to consumers; available in readable formats and necessary languages; and reasonably accessible to consumers with disabilities. **Subsection (b)(2)** requires that the Pre-use Notice be presented prominently and conspicuously before using ADMT; and **subsection (b)(3)** requires that the Pre-use Notice be presented in the manner in which the business primarily interacts with the consumer.

Subsections (b)(1)–(3) are necessary to ensure that consumers will receive the required information in ways that are easy for them to access and understand. This subsection also is necessary to provide clear requirements and guidance to businesses about how to provide a Pre-use Notice, and to enable consumers to make informed choices about whether and how to exercise their rights to opt-out of and access ADMT.

Subsection (c) identifies all the information that must be included in a Pre-Use Notice. This subsection is necessary to ensure that consumers are consistently apprised of the most meaningful pieces of information necessary to inform their decisions about whether to exercise their opt-out and access rights. It also includes tailored exceptions for businesses using ADMT for limited purposes, which balances transparency for consumers against businesses' needs to protect consumers' personal information and businesses' own information systems from

security incidents, fraud, and other negative impacts. It benefits businesses by setting forth clear requirements and guidance about what businesses must include in the Pre-use Notice and benefits consumers by providing consumers with the information necessary to make an informed decision about whether to exercise their opt-out and access rights with respect to ADMT.

Specifically, **subsection (c)(1)** requires the Pre-use Notice to include, in plain non-generic language, the business's purpose for using the ADMT. It also provides that, for training uses of ADMT, the business must identify the specific uses for which the ADMT is capable of being used and the categories of personal information, including any sensitive personal information, that the business plans to process for these training uses. **Subsection (c)(2)** requires the Pre-use Notice to include: a description of consumer's the right to opt-out of ADMT and how to submit their opt-out request; or any relevant exception to providing the opt-out right; and, if the business is relying upon the human appeal exception, how consumers may submit their appeal. If the business is relying on an exception, it must be identified. **Subsection (c)(3)** requires the Pre-use Notice to include a description of the consumer's right to access ADMT and how to submit their access request; it also clarifies that the description of the right to access ADMT does not apply to the use of ADMT solely for training uses as set forth in subsection 7200(a)(3).

Subsections (c)(1)–(3) are necessary to ensure that consumers are aware of why the business is seeking to use ADMT with respect to them and that they have rights to opt-out of and access ADMT. Without this information, consumers may be unaware that ADMT is being used with respect to them or that they can exercise their CCPA rights to prevent businesses from using the ADMT or, if consumers choose to proceed, that they will be able to access more information about the business's use of that technology.

Subsection (c)(4) requires the Pre-use Notice to include that the business cannot retaliate against consumers for exercising their CCPA rights. This subsection is necessary to ensure that consumers know that they have a right to non-retaliation under the CCPA, and that businesses cannot discriminate against consumers when they exercise their opt-out and access rights. Without this subsection, consumers may be wary of exercising their CCPA rights, particularly in employment contexts, if they are under the misapprehension that a business could retaliate against them for doing so.

Subsections (c)(5)(A) and **(B)** require the Pre-use Notice to include a plain language explanation of how the ADMT works, including (1) the logic of the ADMT and key parameters that affect its output; and (2) the intended output of the ADMT and how the business plans to use it, as well as the role of any human involvement. To provide guidance for businesses and consumers, it also provides illustrative examples of ADMT outputs and how a human may be involved. These subsections are necessary to ensure that consumers have a meaningful understanding of how the ADMT would work so they can decide whether to opt-out or proceed, and whether to access more information about how that technology was used with respect to them. Without this information, consumers would lack sufficient understanding of the ADMT to determine whether to exercise their CCPA rights with respect to the use of that technology.

Subsection (c)(5)(C) clarifies that a business relying upon the security, fraud prevention, and safety exception is not required to include information that would compromise its security, fraud prevention, and safety efforts. This subsection is necessary to ensure that businesses providing information to consumers about how their ADMT works are not required to provide information that would compromise security, fraud prevention, or safety. The harms that consumers suffer as a result of unauthorized access to their personal information, fraud, and threats to their physical safety are significant, such as identity theft, economic harm, and physical, psychological, and reputational harm. Therefore, it is important that these regulations balance providing meaningful information to consumers and preserving businesses' ability to protect themselves and consumers: (1) from security incidents that compromise personal information; (2) from malicious, deceptive, fraudulent, or illegal actions; and (3) from threats to consumers' physical safety. Public comments received by the Agency during preliminary rulemaking also highlight the importance of this balance when requiring businesses to provide information to consumers.

Subsection (c)(5)(D) clarifies that **subsection (c)(5)**'s requirement does not apply to a business's use of ADMT solely for training uses as set forth in subsection 7200(a)(3). This subsection is necessary to clarify that businesses are not required to provide information about how the ADMT would work for training uses of ADMT. This approach balances transparency for consumers and the burden on businesses to provide this information at this time.

Subsection (d) clarifies that a business may consolidate its Pre-use Notices in different ways (e.g., a single ADMT for multiple purposes or multiple ADMTs for a single purpose), provided that the consolidated notices include the information required by Article 11 for each of the business's proposed uses. This regulation is necessary to clarify that a business can meet its obligations under this section without providing separate Pre-use Notices for each of the business's uses of ADMT with respect to that consumer. It provides flexibility and reduces the burden on businesses. It also benefits consumers by ensuring that they consistently receive the most meaningful pieces of information necessary to inform their decisions about whether to exercise their opt-out and access rights without being overwhelmed by the number of notices they receive.

§ 7221. Requests to Opt-Out of ADMT.

The purpose of section 7221 is to operationalize consumers' right to opt-out of a business's use of ADMT.

Subsection (a) explains that a business must provide consumers with the ability to opt-out of the business's use of ADMT if the ADMT is used for a significant decision, extensive profiling, or training uses of ADMT, as those terms are defined in section 7200, subsection (a). Each of these uses of ADMT presents significant risk to consumers' privacy, and thus, warrants a consumer's ability to opt-out of these uses of ADMT. For further discussion of the privacy risks to consumers arising from these uses of ADMT, please see the discussion of subsections 7150(b)(3)–(4) above.

This regulation is necessary to identify when a business must provide consumers with the ability to opt-out of their use of ADMT, specifically when the use of ADMT presents significant risk to consumers' privacy. It also is necessary to further the intent and purposes of the CCPA, including to provide consumers with meaningful control over their personal information. (*See* Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3.) It is informed by approaches in federal, state, and international contexts. (*See,* e.g., *supra* notes 71–73.)

Subsection (b) identifies exceptions to the consumer's right to opt-out of ADMT. The exceptions are tailored to different use cases and seek to further protect consumers' privacy while giving attention to the impact on businesses. They align with CCPA's direction to strengthen consumer privacy while giving attention to the

impact on business and innovation. (*See* Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3.)

Subsection (b) is necessary to provide clarity and guidance to businesses about when they do not need to provide consumers with the ability to opt-out of their use of ADMT. Specifically, **subsection (b)(1)** explains that a business does not need to provide an opt-out of ADMT when it uses the ADMT solely for security, fraud prevention, and safety (applicable only to work/educational profiling and public profiling). This subsection is consistent with similar exemptions in the existing right to limit the use of sensitive personal information. This exception is necessary to preserve businesses' ability to protect themselves and consumers from: (1) security incidents that compromise personal information; (2) malicious, deceptive, fraudulent, or illegal actions; and (3) threats to consumers' physical safety. It is informed by public comments received by the Agency during the preliminary rulemaking. As noted above regarding subsection 7220(c)(5)(C), consumers suffer significant harms as a result of (1) unauthorized access to their personal information; (2)fraud; and (3) threats to their physical safety. Therefore, it is important that these regulations balance control for consumers regarding how their personal information is used and preserving businesses' ability to protect themselves and consumers.

Subsection (b)(2) explains that a business does not need to provide an opt-out of ADMT when it provides consumers with the ability to appeal a decision to a qualified human reviewer who has the authority to overturn the decision (applicable only to significant decisions). **Subsections (b)(2)(A)** and **(b)(2)(B)** explain what businesses must do to qualify for the exception. Specifically, businesses must ensure that the human reviewer consider relevant information provided by a consumer, provide a method of appeal that is easy to execute, and respond to requests to appeal in accordance with section 7021. This subsection is necessary to provide clarity and guidance to businesses on how to incorporate human review into their use of ADMT for significant decisions. It is also necessary to give businesses flexibility regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them.

Subsections (b)(3)–(5) respectively explain that a business does not need to provide an opt-out of ADMT when it uses ADMT for admission, acceptance, or hiring decisions; for allocation or assignment of work and compensation decisions; or for work or educational profiling, provided that the business's use of the ADMT is

necessary for these respective purposes, that the business has evaluated its use of ADMT to ensure it works as intended for the business's proposed use and does not discriminate; and that the business has implemented accuracy and nondiscrimination safeguards. These exceptions are necessary to provide flexibility for businesses and reduce burdens on them where it may not be feasible to provide consumers with an opt-out from businesses' use of ADMT, while providing protections against improper deployment and use of the ADMT and discrimination upon the basis of protected classes that can result from businesses' use of ADMT. These exceptions are informed by public comments received by the Agency during the preliminary rulemaking regarding potential challenges in providing the ability to opt-out in certain contexts, such as same-day hiring opportunities. These subsections also provide flexibility for businesses that obtain their ADMT from another person; each permits the business to instead review that person's evaluation of the ADMT for any relevant requirements or limitations rather than requiring the business to conduct its own evaluation of the technology.

Subsection (b)(6) clarifies that the exceptions in subsections (b)(1)–(5) do not apply to profiling for behavioral advertising or training uses of ADMT. This subsection is necessary to avoid any confusion among businesses that might misunderstand the application of these exceptions and seek to use them to avoid providing consumers with their right to opt-out of ADMT for behavioral advertising or training uses of ADMT. It is also necessary because the exceptions described above are meant to address circumstances raised by public comments in which it may be practically infeasible to provide consumers with the ability to opt-out (for example, the use of ADMT to fulfill same-day job placements), which are not applicable to the profiling for behavioral advertising or training contexts.

Subsection (c) requires that businesses provide two or more methods for submitting opt-out of ADMT requests. It also clarifies that at least one method must reflect the manner in which the business primarily interacts with the consumer. This subsection is necessary to fulfill the Agency's statutory obligation to issue regulations governing opt-out rights with respect to businesses' use of ADMT, to provide necessary clarity and guidance to businesses regarding how to provide consumers with the ability to opt-out of businesses' use of ADMT, and to ensure that consumers receive meaningful access to their right to opt-out of ADMT. This subsection is consistent with similar requirements for the opt-out of sale/sharing and the right to limit the use of sensitive personal information. (*See* subsections 7026(a), 7027(b).) It benefits businesses by enabling them to leverage their existing

CCPA opt-out methods and extend them to the right to opt-out of ADMT, and by providing businesses with flexibility to determine how to receive opt-out of ADMT requests. This subsection also benefits consumers by ensuring that at least one of the methods for submitting requests reflects the manner in which the consumer interacts with the business.

Specifically, **subsection (c)(1)** requires businesses to provide an opt-out link titled, "Opt-out of Automated Decisionmaking Technology," in the Pre-use Notice if the business interacts with consumers online. This ensures that consumers interacting with a business online have an easy way to exercise their opt-out of ADMT right. **Subsections (c)(2)–(3)** are illustrative and provide guidance to businesses on other acceptable opt-out methods consisting of standard methods of communication. Lastly, **subsection (c)(4)** clarifies that a cookie banner or similar notification about cookies does not necessarily comply with the requirements of subsection (c)(1) for website methods of submission. To comply, the cookie banner or similar notification must notify the consumer about the right to opt-out of ADMT in specific terms. These subsections are necessary to make sure that consumers are aware of their right to opt-out of ADMT and can easily exercise that right, to ensure that businesses do not choose obscure methods for consumers to submit requests, and to address observations in the marketplace about businesses inappropriately using cookie banners or controls. Subsections (c)(1)–(4) also promote consistency in how consumers can opt-out of ADMT with how consumers can opt-out of sale/sharing and how they can exercise their right to limit under existing regulations. (*See* subsections 7026(a)(1)–(4), 7027(b)(1)–(4).)

Subsections (d)–(f) provide clarity and guidance to businesses regarding how to provide consumers with the ability to opt-out of the businesses' use of ADMT and explain that businesses are not permitted to use dark patterns or impose unnecessary obstacles to consumers seeking to exercise their opt-out of ADMT right. Specifically, **subsection (d)** requires that methods for submitting requests to opt-out of ADMT be easy to execute, require minimal steps, and comply with 7004. **Subsection (e)** prohibits requiring a consumer to create an account or provide additional information beyond what is necessary to direct the business to opt-out the consumer. **Subsection (f)** prohibits requiring a verifiable consumer request but permits a business to ask for information necessary to complete the request. These subsections are necessary to fulfill the Agency's statutory obligation to issue regulations governing opt-out rights with respect to businesses' use of ADMT and to clarify for businesses how to process requests to opt-out of ADMT. These

subsections also promote consistency with existing requirements for the right to opt-out of sale/sharing and the right to limit; this enables businesses to leverage their existing processes for CCPA rights and extend them to the right to opt-out of ADMT. (*See* subsections 7026(b)–(d), 7027(c)–(e).) It also benefits businesses by providing clear guidance about how businesses must provide consumers with the ability to opt-out of businesses' uses of ADMT, and benefits consumers by ensuring that they can easily exercise their right to opt-out of ADMT.

Subsection (g) permits a business to deny a request that it has a good-faith, reasonable, and documented belief is fraudulent. It also requires the business to inform the requestor that it will not comply with the request and provide an explanation of why it believes the request is fraudulent. This subsection is necessary to fulfill the Agency's statutory obligation to issue regulations governing opt-out rights with respect to businesses' use of ADMT and prevent harm to both businesses and consumers. It also provides necessary clarity and guidance to businesses regarding how to comply with consumers' requests to opt-out of their use of ADMT. In addition, it is consistent with existing requirements of businesses and protections for consumers with respect to their exercise of other existing CCPA rights. (*See* subsections 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.

Subsection (h) requires that the business provide a means by which the consumer can confirm that their opt-out of ADMT request has been processed. This subsection is necessary to promote transparency and consumer understanding of the outcome of their request. It is also consistent with the requirements relating to the right to opt-out of sale/sharing and the right to limit. (*See* subsections 7026(g), 7027(h).) Rather than requiring the business to confirm receipt of the request to opt-out of ADMT, which may create friction in the consumer's user experience, the Agency determined that imposing a standard that gives flexibility to the business regarding how to display the status of the consumer's request addresses the need for transparency with a lesser burden to the business to craft the means in accordance with how it manages other CCPA requests.

Subsection (i) permits a business to provide consumers with the choice of allowing specific uses of ADMT, so long as the business also offers a single option to opt-out of all ADMT subject to subsection (a). The requirement to provide a single option to opt-out of all ADMT subject to subsection (a) is necessary to prevent consumer

confusion and to prevent businesses from presenting options to consumers in a strategic manner intended to curtail exercise of the right to opt-out of ADMT. This subsection is also consistent with similar requirements for other CCPA rights (*see* subsections 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. This subsection benefits both businesses and consumers by allowing requests to opt-out of ADMT, where appropriate, to be targeted to limit only certain uses of ADMT.

Subsection (j) permits a consumer to submit requests using an authorized agent if the consumer provides signed permission to the agent. It also allows a business to deny an authorized agent's request if the agent does not provide the signed permission to the business. This subsection is necessary to ensure that consumers can use authorized agents to facilitate their requests to opt-out of ADMT, similar to what they can already do for their other CCPA rights. (*See* subsection 7026(j); subsection 7027(j).) In addition, by promoting consistency with how businesses must already treat consumer requests to exercise their other CCPA rights via authorized agents, this regulation also benefits businesses because businesses can leverage their existing authorized-agent processes and extend them to the opt-out of ADMT.

Subsection (k) requires that businesses wait at least 12 months before asking consumers that opted out of ADMT to consent to their use of that ADMT. This subsection is necessary to ensure that consumers that have opted out of ADMT are not inundated with requests to consent to that use of ADMT. This subsection benefits consumers by ensuring their right to opt-out of ADMT is respected and that they are not repeatedly asked to consent after opting out. This subsection is consistent with requirements for other CCPA rights, which benefits businesses by enabling them to leverage existing consent processes and extend them to the right to opt-out of ADMT. (*See* subsection 7026(k); subsection 7027(*l*).)

Subsection (*l*) prohibits businesses from retaliating against consumers who exercised their right to opt-out of ADMT. This subsection facilitates compliance with the statutory prohibition against retaliation in Civil Code section 1798. 125, subdivisions (a)–(b), and Article 7 of the existing regulations. Including the statutory and existing regulatory requirements of non-retaliation and non-discrimination is necessary for clarity because it consolidates the relevant requirements for the right to opt-out of ADMT in one place.

Subsection (m) states that when a consumer has opted out of ADMT before the business initiated the processing, the business must not initiate processing of the consumer's personal information using that ADMT. This subsection is necessary to clarify businesses' obligations when complying with a request to opt-out of ADMT that has been submitted before the business initiated the processing.

Subsection (n) states that if a consumer submitted an opt-out of ADMT request after the business initiated processing, the business must cease processing the consumer's personal information using that ADMT as soon as possible, and no later than 15 business days after receiving the request. It also prohibits the business from using or retaining any personal information previously processed by that ADMT and requires the business to notify all other persons to whom it disclosed information using that ADMT that the consumer has opted out and instructing them to comply with the opt-out within the same time frame. This subsection is necessary to clarify businesses' obligations with respect to requests to opt-out of ADMT that have been submitted after the business initiated the processing. It is also necessary to protect consumers' right to opt-out of ADMT, by ensuring their requests are communicated to, and complied with by, the service providers, contractors, or other persons to whom their personal information has been disclosed or made available for processing using ADMT. This subsection also is consistent with the timeframe requirements for other CCPA opt-out rights, which benefits both businesses and consumers by promoting a clear standard for when opt-out rights must be processed under the CCPA. (*See* subsections 7026(f), 7027(g).)

§ 7222. Requests to Access ADMT.

The purpose of this section is to operationalize consumers' right to access with respect to a business's use of ADMT.

Subsection (a) requires businesses to provide consumers with the ability to access information about the business's use of ADMT for significant decisions and extensive profiling. This subsection is necessary to clarify which uses of ADMT are subject to the requirements set forth in this section for requests to access ADMT. Providing access to information about how businesses use ADMT for significant decisions and extensive profiling benefits consumers by providing them with transparency and control over their personal information.

Subsection (a)(1) states that businesses using ADMT solely for training uses are not required to provide a response to a consumer's request to access ADMT. The subsection explicitly excludes training uses of ADMT to avoid confusion for businesses about which uses of ADMT are subject to the access-ADMT requirements. It excludes training uses of ADMT to limit the burden on businesses and streamline implementation of the right to access ADMT at this time.

Subsection (b) clarifies for businesses and consumers what businesses must provide in response to a request to access ADMT. Specifically, **subsection (b)(1)** requires that businesses provide a plain language explanation of the specific purpose for which the business used ADMT with respect to the consumer, and prohibits describing the purpose in general terms, such as "to improve our services." This subsection is necessary to clarify that consumers need to know the specific purpose for which the business used ADMT with respect to them as part of consumers' right to access ADMT. The prohibition against using general terms to describe purposes is necessary to prevent businesses using vague language about their use of ADMT, which undermines consumers' exercise of their access ADMT right and undercuts consumers' ability to understand why ADMT was used with respect to them. Without this subsection, consumers would lack sufficient understanding about why a business processed their personal information using that ADMT, as well as the potential impact of the business's use of ADMT with respect to them.

Subsection (b)(2) requires that a business provide a plain language explanation of the output of the ADMT with respect to the consumer. If the business has multiple outputs with respect to the consumer, this subsection also gives the business the option to provide a simple and easy-to-use method for consumers to access those outputs. This subsection is necessary to implement the statutory direction that businesses provide meaningful information about the logic involved in the ADMT's decisionmaking process, as well as a description of the likely outcome of the process with respect to the consumer. A consumer must know the output of the ADMT with respect to them to understand how the logic of the ADMT was applied to them and the role of the ADMT as part of the business's decisionmaking process. In addition, if a consumer identifies discrepancies or inaccuracies in the output, they can exercise their other CCPA rights, such as the right to correct, as necessary to correct the issue. Provision of the output of the ADMT is therefore necessary to ensure that consumers have meaningful control over their personal information, including having sufficient information to determine whether to exercise other

CCPA rights. This requirement is consistent with the federal and international guidance and academic scholarship on explainability for ADMT, as well as with approaches in certain decisionmaking contexts.[79]

Subsection (b)(3) requires that a business provide a plain language explanation of how the business used the output with respect to the consumer. Specifically, **subsection (b)(3)(A)** states that if the business used the output to make a significant decision concerning a consumer, this explanation must include the role the output played in the business's decision and the role of any human involvement. **Subsection (b)(3)(A)(i)** states that if a business is planning to use the output to make a significant decision, this explanation must also include how the business plans to use the output to make a decision, including the role of human involvement. Similarly, **subsection (b)(3)(B)** requires that a business using ADMT for extensive profiling explain the role the output played in the evaluation that the business made with respect to the consumer. **Subsection (b)(3)(B)(i)** states that if a business is planning to use the output to evaluate the consumer, the business's explanation also must include how the business plans to use the output to evaluate the consumer. **Subsection (b)(3)** is necessary to implement the statutory requirement that businesses provide a description of the likely outcome of their decisionmaking process with respect to the consumer in response to access ADMT requests. For consumers to meaningfully understand the outcome of a decisionmaking process, they must know how a business used, or plans to use, the ADMT's output in a decision or evaluation. Otherwise, consumers would be provided only the output without important contextual information about how that output was, or would be used, with respect them. In addition, in the context of significant decisions, requiring that businesses explain the role of human involvement ensures that consumers understand to what extent automated versus human decisionmaking played a role in the outcome of the decisionmaking process.

Subsection (b)(4) requires the business to provide a plain language explanation of how the ADMT worked with respect to the consumer. **Subsection (b)(4)(A)** requires that the business provide an explanation of how the logic, including its assumptions

---

[79] *See supra* notes 71, 73. *See also* 15 U.S.C. §§ 1681m(a), 1691(d)(2)(A)–(B); 12 C.F.R. § 1022.73(a)(1)(ix); *Appendix H to Part 1022 - Model Forms for Risk-Based Pricing and Credit Score Disclosure Exception Notices*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/rules-policy/regulations/1022/h/#a-iii; *Using Consumer Reports for Credit Decisions: What to Know About Adverse Action and Risk-Based Pricing Notices*, FED. TRADE COMM'N (Nov. 2016).

and limitations, was applied to the consumer. **Subsection (b)(4)(B)** requires that the business provide the key parameters that affected the ADMT and how they were applied to the consumer. This subsection is necessary to implement the statutory direction that businesses provide meaningful information about the logic involved in the decisionmaking process in response to access requests. For information about the logic to be meaningful to a consumer, the consumer must know how the logic was actually applied to them, including the relevant assumptions and limitations of that logic, and the relevant parameters that affected the output. This provides important context for consumers to understand how the ADMT actually worked as part of a significant decision or extensive profiling with respect to them. This requirement is consistent with the federal and international guidance and academic scholarship on explainability for ADMT, as well as with the approach to providing meaningful information to consumers in the credit-score context, where creditors provide consumers with the key factors that adversely affected their credit score.[80]

Subsection (b)(4)(C) states that businesses may provide the range of possible outputs or aggregate output statistics and provides an example of how to do so. This subsection is necessary to provide guidance to businesses about how to provide additional meaningful information to consumers about how the ADMT worked with respect to them versus other consumers. This option provides flexibility for businesses and guidance about information that businesses can choose to incorporate in their responses to access ADMT requests.

Lastly, **subsection (b)(4)(D)** states that a business relying upon the security, fraud prevention, and safety exception to providing a consumer with the ability to opt-out of ADMT is not required to provide information that would compromise its use of ADMT for security, fraud prevention, or safety purposes. This subsection is necessary to clarify that businesses are not required to provide information in an access request that would compromise their security, fraud prevention, or safety uses of ADMT. As noted above regarding subsection 7220(c)(5)(C) and subsection 7221(b)(1), consumers suffer significant harms as a result of (1) unauthorized access to their personal information; (2) fraud; and (3) threats to their physical safety. Therefore, it is important that these regulations balance providing meaningful information to consumers and preserving businesses' ability to protect themselves

[80] *See id.*

and consumers by avoiding potentially harmful disclosures of information in response to access ADMT requests.

Subsection (b)(5) requires that a business provide a plain language explanation to consumers that the business is prohibited from retaliating against consumers for exercising their CCPA rights. It also requires the business to provide instructions for how the consumer can exercise their other CCPA rights. This subsection further clarifies that these instructions must include any links to online request forms or portals for making such requests. This subsection is necessary to ensure that consumers are aware that they can exercise other CCPA rights, such as the right to correct, to address potential issues they identify in the access response (such as inaccurate information), and that they can do so without fear of retaliation. It also provides flexibility for businesses, clarifying that they may comply with the instructions requirement by providing a link that takes the consumer directly to the section of the business's privacy policy that contains the required information. The subsection also specifies that the business cannot link the consumer to another section of the policy or to a place that requires the consumer to scroll through other information. This is necessary to ensure that the consumer can clearly distinguish the pertinent information that must be provided to them.

Subsection (c) requires that methods to submit access ADMT requests are easy to use and do not use dark patterns. It states that businesses may use existing methods to submit requests to know, delete, or correct, as set forth in section 7020, for requests to access. This subsection is necessary to clarify how to operationalize submission of requests to access ADMT. It provides a performance-based standard that gives businesses flexibility regarding how to set up submission of access ADMT requests while addressing consumers' needs to be able to effectively submit consumer requests. It also prohibits the use of dark patterns to make clear that businesses cannot use methods to submit requests that subvert or impair consumers' choice about whether to exercise their right to access ADMT. It also provides guidance to businesses that they may use their existing methods for submission of other CCPA requests to comply with this standard, which makes the requirement less burdensome.

Subsection (d) requires verification of the identity of the person making the request to access ADMT as set forth in Article 5, and states that if a business cannot verify their identity, the business must inform the requestor that it cannot verify their identity. This subsection is necessary to clarify that a business must verify the

requestor, which balances the consumer's right to access ADMT with the consumer's interest in preventing the disclosure of their personal information to unauthorized persons. It cross-references Article 5 so that businesses can easily identify where in the regulations they can find the verification requirements for requests to access ADMT. This subsection is consistent with the verification requirements for other CCPA rights, which benefits businesses by enabling them to leverage their existing verification processes and extend them to the right to access ADMT.

Subsection (e) states that if a business denies a verified access request because of a conflict with other laws or an exception to the CCPA, the business must inform the requestor and explain the basis of the denial, unless prohibited from doing so by law. If the request is denied only in part, the business must disclose the other information sought by the consumer. This subsection is necessary because it provides direction to a business on what to communicate to consumers when it denies a request on these grounds. This benefits consumers by giving them greater transparency concerning the business's process for handling their access requests and provides consumers with an opportunity to cure any defects in their request as well as a potential basis for contesting the denial. It also benefits consumers by prohibiting businesses from treating consumers' requests in an all-or-nothing fashion. This regulation is consistent with requirements for denying requests to exercise other CCPA rights, which benefits businesses by enabling them to leverage their existing denial processes and extend them to the right to access ADMT.

Subsection (f) requires that businesses use reasonable security when transmitting the requested information to the consumer. This subsection is necessary to protect consumers' personal information during transmittal. This subsection is consistent with similar security requirements for other CCPA rights, such as the right to know, which benefits businesses by enabling them to leverage their existing security processes and extend them to the right to access ADMT. (*See* subsection 7024(f).)

Subsection (g) allows businesses that maintain password-protected accounts with consumers to comply with a request to access ADMT by utilizing a secure self-service portal for consumers to access, view, and receive a portable copy of the requested information. It requires that the portal fully disclose the requested information that the consumer is entitled to receive about the business's use of ADMT with respect to them under the CCPA and these regulations, utilize

reasonable data security controls, and comply with the verification requirements set forth in Article 5 of these regulations. This regulation is necessary to provide businesses with discretion and flexibility in responding to consumers' requests in a cost-effective manner while ensuring that businesses comply fully with consumers' requests in a secure fashion. It also provides clarity regarding how businesses are to respond to consumer requests and is consistent with similar provisions for the right to know, which enables businesses to leverage existing CCPA request processes and extend them to the right to access ADMT. (*See* subsection 7024(g).)

Subsection (h) requires that service providers or contractors provide assistance to businesses in responding to access ADMT requests, including by providing personal information in their possession or enabling the business to access that information. This subsection is necessary to clarify the requirements of a service provider and contractor when a consumer makes a request to access ADMT of the business it is servicing. It provides service providers and contractors with clear guidance about what is required of them, while preventing a business from avoiding the obligation to provide information in response to requests to access ADMT by utilizing service providers or contractors.

Subsection (i) clarifies that businesses that use ADMT more than four times within a 12-month period with respect to a consumer may provide aggregate-level responses to a consumer's request to access ADMT. The subsection further explains how information required in response to an access ADMT request can be aggregated, such as providing a summary of the outputs with respect to the consumer over the preceding 12 months; the key parameters that, on average over the preceding 12 months, affected the outputs with respect to the consumer; and a summary of how those parameters generally applied to the consumer. This subsection is necessary to provide businesses the flexibility to consolidate responses to access ADMT requests when they are using ADMT repeatedly with respect to a consumer, while still providing consumers with the ability to access ADMT. It clarifies how businesses can meaningfully provide the information requested by a consumer in this scenario. It also provides guidance on how businesses can consolidate the information into aggregate-level responses.

Subsection (j) prohibits businesses from retaliating against a consumer for exercising their right to access ADMT. This subsection facilitates compliance with the statutory prohibition against retaliation in Civil Code section 1798.125, subdivisions (a)–(b), and Article 7 of the existing regulations. Including the statutory

and existing regulatory requirements of non-retaliation and non-discrimination is necessary for clarity because it consolidates the relevant requirements for the right to access ADMT in one place, which benefits businesses by making the requirements easier to follow and understand.

Subsection (k) requires a business that uses ADMT to make an adverse significant decision concerning a consumer to provide the consumer with notice of their right to access ADMT as soon as feasibly possible and no later than 15 business days from the date of the adverse significant decision. **Subsection (k)(1)** states that an adverse significant decision is a significant decision that resulted in a consumer, acting in their capacity as a student, employee, or independent contractor, being denied an educational credential; having their compensation decreased; being suspended, demoted, terminated, or expelled; or resulted in a consumer being denied financial or lending services, housing, insurance, criminal justice, healthcare services, or essential goods or services. This subsection is necessary to clarify when businesses must provide notice (i.e., what is an adverse significant decision) so that businesses know when the requirement applies. It also clarifies that businesses must provide the notice to consumers as soon as feasibly possible but no later than 15 days from the date of the adverse significant decision, which balances the consumer's need to know the information as soon as possible with the potential burden on businesses to provide this notice. Requiring businesses to provide consumers with notices of adverse actions taken against them is also consistent with approaches taken in other contexts, such as credit decisions.[81]

Subsection (k)(2) states that a business must include in that notice: that the business used ADMT to make a significant decision with respect to the consumer; that the business is prohibited from retaliating against consumers for exercising their CCPA rights; that the consumer has a right to access ADMT and how the consumer can exercise their access right; and, if applicable, that the consumer can appeal the decision and how they can submit their appeal and any supporting documentation.

---

[81] *See, e.g.*, 15 U.S.C. §§ 1681m(a), 1691(d)(2)(A)–(B); 12 C.F.R. § 1022.73(a)(1)(ix); *Appendix H to Part 1022 - Model Forms for Risk-Based Pricing and Credit Score Disclosure Exception Notices*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/rules-policy/regulations/1022/h/#a-iii; *Using Consumer Reports for Credit Decisions: What to Know About Adverse Action and Risk-Based Pricing Notices*, FED. TRADE COMM'N (Nov. 2016).

This subsection is necessary to ensure that consumers have sufficient information to exercise their right to access ADMT when it is particularly important for them (i.e., when an adverse significant decision has been made). Each part of the notice provides important information to the consumer so they can determine whether to exercise their right to access ADMT: they need to know that ADMT was used to make an adverse significant decision with respect to them; that they have the right to access ADMT and how to exercise it; that they cannot be retaliated against for exercising their CCPA rights; and if they want to appeal the decision as applicable, how they can do so. This subsection is also necessary to ensure that consumers are aware of their right to access ADMT under circumstances when an adverse significant decision was made significantly after they received a Pre-use Notice (e.g., if they were terminated from their job two years after receiving the Pre-use Notice).

Lastly, **subsection (k)(3)** states that businesses can provide this notice to consumers with their notification of the adverse significant decision. The subsection provides the example that if a business ordinarily notifies consumers of termination decisions via email, the business can include the information required by subsection (k)(2) in that notification, provided that the notice overall complies with the requirements for disclosures in subsections 7003(a)–(b). The subsection also states that a business may provide a separate contemporaneous notice of the right to access ADMT that includes the information in subsection (k)(2). This subsection is necessary to provide clarity and guidance to businesses about when they can consolidate notices—specifically, that businesses can provide the information required by subsection (k)(2) to consumers in their notice of the adverse significant decision to consumers. It also clarifies that the business may, as an alternative, provide this additional notice contemporaneously, to address instances where the business does not want to consolidate notices. The subsection provides flexibility for businesses, which reduces the burden on businesses and potentially reduces the number of notices consumers will receive, while still ensuring that consumers receive the information necessary to decide whether to exercise their right to access ADMT or other CCPA rights, such as the right to correct.

ARTICLE 12. INSURANCE COMPANIES

Civil Code section 1798.185, subdivision (a)(21), requires the Agency to review existing Insurance Code provisions and regulations relating to consumer privacy (but not insurance rates or pricing) to determine whether any provisions within the

Insurance Code afford consumers greater privacy protection than those found within the CCPA. Following the completion of this evaluation, the Agency must promulgate a regulation that applies the more privacy protective provisions of the CCPA to insurance companies.

As an initial matter, sections 7270 and 7271 set the baseline for the regulations governing the insurance industry. These regulations clarify the existing requirements and respond to concerns regarding the personal information collected, used, processed, or retained by insurance companies that are not subject to the Insurance Code and other laws, such as the federal Gramm-Leach-Bliley Act. They do not introduce new laws nor amend existing legal rights or requirements.

§ 7270. Definition of Insurance Company.

Subsection (a) defines the term "insurance company," pursuant to the California Insurance Code. This subsection is necessary to clarify who the regulations apply to and help eliminate any misunderstanding or confusion related to the term. It assists businesses in implementing the regulation, and thereby increases the likelihood that consumers will enjoy the benefits of the rights provided them by the CCPA.

§ 7271. General Application of the CCPA to Insurance Companies.

Subsection (a) clarifies that insurance companies meeting the definition of "businesses" under the CCPA shall comply with the CCPA regarding any personal information collected, used, processed, or retained that is not subject to the California Insurance Code.

This subsection is necessary to address any ambiguity regarding insurance companies' obligations under the CCPA. It acknowledges that the CCPA and Insurance Code may overlap in their jurisdiction and delineates the boundary between the two legal frameworks. While the Insurance Code applies to personal information collected, used, processed, or retained in connection with an insurance transaction, any personal information outside this scope, as well as other laws exempt from the CCPA, falls under the CCPA's purview.

The need for this clarification comes from the different scope of the CCPA and the Insurance Code. The CCPA generally covers a broader range of consumers, businesses, and personal information. (*See* Civ. Code, § 1798.140, subds. (*l*), (d), and (v)(1); Ins. Code, § 791.02, subds. (i), (*l*), and (m).) Specifically, the CCPA provides

rights to all California residents, while the Insurance Code applies only to California residents that are involved in insurance transactions. (*See* Civ. Code, § 1798.140, subd. (i): Ins. Code, § 791.02, subd. (i).) The CCPA also covers more businesses as it applies to all entities that meet the definition of "business," whereas the Insurance Code is limited to insurance institutions, agents, and insurance-support organizations that collect and maintain information about insurance transactions. (*See* Civ. Code, § 1798.140, subd. (d); Ins. Code, § 791.02, subd. (*l*).)

Furthermore, the CCPA covers more personal information than the Insurance Code. Personal information is defined broadly under the CCPA and includes all information that is reasonably capable of being associated with or linked to a particular consumer or household. (*See* Civ. Code, § 1798.140, subd. (v)(1)). In contrast, the Insurance Code applies to "individually identifiable information gathered in connection with an insurance transaction from which judgments can be made." (*See* Ins. Code, § 791.02, subds. (m) and (s).) Accordingly, the state of the law is that insurance companies must comply with the Insurance Code requirements for any information subject to the Insurance Code, but the CCPA applies to any information outside of the insurance transaction.

By clarifying the circumstances under which the CCPA applies, this regulation allows insurance companies to evaluate how the CCPA would apply in situations where the Insurance Code does not apply. This clarification helps insurance companies understand their obligations, thereby reducing the risk of non-compliance and improving operational efficiency. It also benefits consumers by explaining that insurance companies must still allow them to exercise their CCPA privacy rights regarding personal information collected, used, processed, or retained outside of an insurance transaction.

Subsection (b) provides two examples that illustrate how subsection (a) works. These examples are necessary to demonstrate where CCPA's jurisdiction begins, and the Insurance Code's jurisdiction ends. They offer businesses guidance on how to apply the law. This subsection benefits both consumers and businesses by providing clear examples of how insurance companies must comply with the CCPA in the collection, use, process, and retention of personal information.

ARTICLE 13. INVESTIGATIONS AND ENFORCEMENT

Change without regulatory effect. The article has been renumbered.

§ 7300. Sworn Complaints Filed with the Agency.

Subsection (a) replaced "may" with "must" to clarify how consumers are to submit sworn complaints to the Agency. This change is necessary to accurately explain to businesses and consumers how sworn complaints are to be filed. It benefits consumers and businesses by providing certainty regarding the Agency's processes.

§ 7302. Probable Cause Proceedings.

Subsection (b) has been revised to clarify that the Agency will provide the alleged violator with notice of the probable cause proceeding. This change is necessary because the notice may come from the Legal Division and not the Enforcement Division. Referring to the Agency provide greater clarity for businesses who may be subject to a probable cause proceeding.

Subsection (c)(1) has been revised to clarify that a probable cause proceeding can be conducted in whole or in part by telephone or videoconference unless the alleged violator requests an in-person or public proceeding. This revision is necessary to make clear that in-person meetings do not need to be open to the public. An alleged violator may request that the proceeding be in-person while also being closed to the public. Also, the change clarifies that there is flexibility for proceedings to be held in whole or in part by telephone or videoconference. This benefits businesses and consumers by maximizing the ways in which people can participate in the proceeding. It increases convenience for the parties and minimizes the costs associated with a public hearing, such as travel and hotel.

Subsection (c)(3) has been revised to replace "participate or appear at" with "attend" because the word "attend" is broader in meaning and inclusive of both attending via telephone or videoconference and attending in person. This change is necessary to make the regulation easier to understand.

Subsection (e) has been deleted to avoid the misimpression that these regulations amend the rules of evidence.

The following sections will be added after completing the Department of Finance review process.

ECONOMIC IMPACT ASSESSMENT / ANALYSIS

TECHNICAL, THEORETICAL, OR EMPIRICAL STUDIES, REPORTS, OR SIMILAR DOCUMENTS RELIED UPON

EVIDENCE SUPPORTING DETERMINATION OF NO SIGNIFICANT STATEWIDE ADVERSE ECONOMIC IMPACT DIRECTLY AFFECTING BUSINESS

REASONABLE ALTERNATIVES TO THE PROPOSED REGULATORY ACTION THAT WOULD LESSEN ANY ADVERSE IMPACT ON SMALL BUSINESS

REASONABLE ALTERNATIVES TO THE PROPOSED ACTION AND REASON FOR REJECTING THOSE ALTERNATIVES