DATA RISK ASSESSMENTS:
AI AND PERSONAL DATA PROCESSING

PART 8 DATA PROTECTION ASSESSMENTS

Rule 8.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 8 is C.R.S. §§ 6-1-108(1), 6-1-1309, and 6-11313. The purpose of the rules in this Part 8 is to provide clarity on the requirements and timing of data protection assessments.

Rule 8.02 SCOPE

A. A data protection assessment shall be a genuine, thoughtful analysis of each Personal Data Processing activity that presents a heightened risk of harm to a Consumer, pursuant to C.R.S. § 6-1-1309(3), that: 1) identifies and describes the risks to the rights of consumers associated with the processing; 2) documents measures considered and taken to address and offset those risks, including those duties required by C.R.S. § 6-1-1308; 3) contemplates the benefits of the Processing; and 4) demonstrates that the benefits of the Processing outweigh the risks offset by safeguards in place.

B. If a Controller conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulation, the assessment shall satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

1. If a data protection assessment conducted for the purpose of complying with another jurisdiction's law or regulation is not similar in scope and effect to a data protection assessment created pursuant to this section, a Controller may submit that assessment with a supplement that contains any additional information required by this jurisdiction.

C. The depth, level of detail, and scope of data protection assessments should take into account the scope of risk presented, the size of the Controller, amount and sensitivity of Personal Data Processed, Personal Data Processing activities subject to the assessment, and complexity of safeguards applied.

D. A "comparable set of Processing operations" that can be addressed by a single data protection assessment pursuant to C.R.S. § 6-1-1309(5) is a set of similar Processing operations including similar activities that present heightened risks of similar harm to a Consumer.

1. Example: The ACME Toy Store chain is considering using in-store paper forms to collect names, mailing addresses, and birthdays from Children that visit their stores, and using that information to mail a coupon and list of age-appropriate toys to each child during the Child's birth month and every November. ACME uses the same Processors and Processing systems for each category of mailings across all stores. ACME must conduct and document a data protection assessment because it is Processing Personal Data from known Children, which is Sensitive Data. ACME can use the same data protection assessment for Processing the Personal Data for the birthday mailing and November mailing across all stores because in each case it is collecting the same categories of Personal Data in the same way for the purpose of sending coupons and age-appropriate toy lists to Children.

Rule 8.03 STAKEHOLDER INVOLVEMENT

A. A data protection assessment shall involve all relevant internal actors from across the Controller's organizational structure, and where appropriate, relevant external parties, to identify, assess and address the data protection risks.

Rule 8.04 DATA PROTECTION ASSESSMENT CONTENT

A. At a minimum, a data protection assessment must include the following information:

1. A short summary of the Processing activity;

2. The categories of Personal Data to be Processed and whether they include Sensitive Data, including Personal Data from a known Child as described in C.R.S. § 6-1-1303(24);

3. The context of the Processing activity, including the relationship between the Controller and the Consumers whose Personal Data will be Processed, and the reasonable expectations of those Consumers;

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

   a. Sources of Personal Data;

   b. Technology or Processors to be used;

   c. Names or categories of Personal Data recipients, including Third Parties, Affiliates, and Processors that will have access to the Personal Data, the processing purpose for which the Personal Data will be provided to those recipients, and categorical compliance processes that the Controller uses to evaluate that type of recipient;

   d. Operational details about the Processing, including planned processes for Personal Data collection, use, storage, retention, and sharing;

   e. Specific types of Personal Data to be processed.

5. The core purposes of the Processing activity, as well as other benefits of the Processing that may flow, directly and indirectly to the Controller, Consumer, other expected stakeholders, and the public;

6. The sources and nature of risks to the rights of Consumers associated with the Processing activity posed by the Processing activity. The source and nature of the risks may differ based on the processing activity and type of Personal Data processed. Risks to the rights of Consumers that a Controller may consider in a data protection assessment include, for example, risks of:

   a. Constitutional harms, such as speech harms or associational harms;

b. Intellectual privacy harms, such as the creation of negative inferences about an individual based on what an individual reads, learns, or debates;

c. Data security harms, such as unauthorized access or adversarial use;

d. Discrimination harms, such as a violation of federal antidiscrimination laws or antidiscrimination laws of any state or political subdivision thereof, or unlawful disparate impact;

e. Unfair, unconscionable, or deceptive treatment;

f. A negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services;

g. Financial injury or economic harm;

h. Physical injury, harassment, or threat to an individual or property;

i. Privacy harms, such as physical or other intrusion upon the solitude or seclusion or the private affairs or concerns of Consumers, stigmatization or reputational injury;

j. Psychological harm, including anxiety, embarrassment, fear, and other mental trauma;

k. Other detrimental or negative consequences that affect an individual's private life, private affairs, private family matters or similar concerns, including actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that Personal Data or other data will not be collected, observed, or used.

7. Measures and safeguards the Controller will employ to reduce the risks identified by the Controller pursuant to 4 CCR 904-3, Rule 8.04(A)(6). Measures shall include the following, as applicable:

a. The use of De-identified Data;

b. Measures taken pursuant to the Controller duties in C.R.S. § 6-1-1308, including an overview of data security practices the Controller has implemented, any data security assessments that have been completed pursuant to C.R.S. § 6-11308(5), and any measures taken to comply with the consent requirements of 4 CCR 904-3, Rule 7; and

c. Measures taken to ensure that Consumers have access to the rights provided in C.R.S. § 6-1-1306.

8. A description of how the benefits of the Processing outweigh the risks identified pursuant to 4 CCR 904-3, Rule 8.04(A)(6), as mitigated by the safeguards identified pursuant to 4 CCR 904-3, Rule 8.04(A)(7).

a. Contractual agreements in place to ensure that Personal Data in the possession of a Processor or other Third Party remains secure; or

b. Any other practices, policies, or trainings intended to mitigate Processing risks.

9. If a Controller is Processing Personal Data for Profiling as contemplated in C.R.S. § 6-11309(2)(a), a data protection assessment of that Processing activity must also comply with 4 CCR 904-3, Rule 9.06;

10. If a Controller is Processing Sensitive Data pursuant to the exception in section 4 CCR 904-3, Rule 6.10, the details of the process implemented to ensure that Personal Data and Sensitive Data Inferences are not transferred and are deleted within twenty-four (24) hours of the Personal Data Processing activity;

11. Relevant internal actors and external parties contributing to the data protection assessment;

12. Any internal or external audit conducted in relation to the data protection assessment, including, the name of the auditor, the names and positions of individuals involved in the review process, and the details of the audit process; and

13. Dates the data protection assessment was reviewed and approved, and names, positions, and signatures of the individuals responsible for the review and approval.

Rule 8.05 TIMING

A. A Controller shall conduct and document a data protection assessment before initiating a Processing activity that Presents a Heightened Risk of Harm to a Consumer, as defined at C.R.S. § 6-1-1309(2)

B. A Controller shall review and update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of Personal Data Processed and level of risk presented by the Processing, throughout the Processing activity's lifecycle in order to: 1) monitor for harm caused by the Processing and adjust safeguards accordingly; and 2) ensure that data protection and privacy are considered as the Controller makes new decisions with respect to the Processing.

C. Data protection assessments containing Processing for Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer shall be reviewed and updated at least annually, and include an updated evaluation for fairness and disparate impact and the results of any such evaluation.

D. A new data Processing activity is generated when existing Processing activities are modified in a way that materially changes the level of risk presented. When a new data Processing activity is generated, a data protection assessment must reflect changes to the pre-existing activity and additional considerations and safeguards to offset the new risk level.

1. Modifications that may materially change the level of risk of a Processing activity may include, without limitation, changes to any of the following:

    a. The way that existing systems or Processes handle Personal Data;

    b. Processing purpose;

    c. Personal data Processed or sources of Personal Data;

    d. Method of collection of Personal Data;

    e. Personal Data recipients;

    f. Processor roles or Processors;

    g. Algorithm applied or algorithmic result; or

    h. Software or other systems used for Processing.

E. Data protection assessments, including prior versions which have been revised when a new data Processing activity is generated, shall be stored for as long as the Processing activity continues, and for at least three (3) years after the conclusion of the Processing activity. Data protection assessments shall be held in an electronic, transferable form.

F. Data protection assessments shall be required for activities created or generated after July 1, 2023. This requirement is not retroactive.

Rule 8.06 ATTORNEY GENERAL REQUESTS

A. A Controller shall make the data protection assessment available to the Attorney General within thirty (30) days of the Attorney General's request.

Rule 9.06 DATA PROTECTION ASSESSMENTS FOR PROFILING

A. Controllers must conduct and document a data protection assessment compliant with C.R.S. § 61-1309 and 4 CCR 904-3, Part 8 before Processing Personal Data for Profiling if the Profiling presents a reasonably foreseeable risk of:

1. Unfair or deceptive treatment of, or unlawful disparate impact on Consumers;

2. Financial or physical injury to Consumers;

3. A physical or other intrusion upon the solitude or seclusion, or private affairs or concerns, of Consumers if the intrusion would be offensive to a reasonable person; or

4. Other substantial injury to Consumers.

B. Profiling under C.R.S. § 6-1-1309(2)(a) and covered by required data protection assessment obligations includes Profiling using Solely Automated Processing, Human Reviewed Automated Processing, and Human Involved Automated Processing.

C. "Unfair or deceptive treatment" as used in C.R.S. § 6-1-1309 and 4 CCR 904-3, Rule 9.06 includes conduct or activity which violates state or federal laws that prohibit unfair and deceptive commercial practices.

D. "Unlawful disparate impact" as used in C.R.S. § 6-1-1309 and 4 CCR 904-3, Rule 9.06 includes conduct or activity which violates state or federal laws that prohibit unlawful discrimination against Consumers.

E. Controllers should consider both the type and degree of potential harm to Consumers when determining if Profiling presents a reasonably foreseeable risk of "other substantial injury" to Consumers as used in C.R.S. § 6-1-1309 and 4 CCR 904-3, Rule 9.06(A). For example, a small harm to a large number of Consumers. may constitute "other substantial injury".

F. If a Controller is Processing Personal Data for Profiling under C.R.S. § 6-1-1309(2)(a), a data protection assessment of that Processing activity must include the elements listed at 4 CCR 9043, Rule 8.04 as well as each of the following as applicable to the assessed reasonably foreseeable risk:

1. The specific types of Personal Data that were or will be used in the Profiling or decision-making process;

2. The decision to be made using Profiling;

3. The benefits of automated processing over manual processing for the stated purpose;

4. A plain language explanation of why the Profiling directly and reasonably relates to the Controller's goods and services;

5. An explanation of the training data and logic used to create the Profiling system, including any statistics used in the analysis, either created by the Controller or provided by a Third Party which created the applicable Profiling system or software;

6. If the Profiling is conducted by Third Party software purchased by the Controller, the name of the software and copies of any internal or external evaluations sufficient to show of the accuracy and reliability of the software where relevant to the risks described in C.R.S. § 6-1-1309(2)(a)(I)-(IV);

7. A plain language description of the outputs secured from the Profiling process;

8. A plain language description of how the outputs from the Profiling process are or will be used, including whether and how they are used to make a decision to provide or deny or substantially contribute to the provision or denial of financial or lending services, housing, insurance, education, enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services;

9. If there is human involvement in the Profiling process, the degree and details of any human involvement;

10. How the Profiling system is evaluated for fairness and disparate impact, and the results of any such evaluation;

11. Safeguards used to reduce the risk of harms identified; and

12. Safeguards for any data sets produced by or derived from the Profiling.

G. If a Controller conducts a data protection assessment which includes an assessment of relevant Profiling for the purpose of complying with another jurisdiction's law or regulation, the assessment shall satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section. A Controller may also submit an assessment with a supplement that contains any additional information required by this regulation.

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.

PROPOSED TEXT OF REGULATIONS

JULY 2024

The original text published in the California Code of Regulations has no underline. Changes are illustrated by single blue underline for proposed additions and single red strikethrough for proposed deletions.

New articles, specifically Article 9 (Cybersecurity Audits), Article 10 (Risk Assessments), Article 11 (Automated Decisionmaking Technology), and Article 12 (Insurance Companies), are not underlined for ease of review.

CPPA

[The following article is new and does not currently exist in the Code of Regulations.]

ARTICLE 10. RISK ASSESSMENTS

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

(a) Every business whose processing of consumers' personal information presents significant risk to consumers' privacy as set forth in subsection (b) must conduct a risk assessment before initiating that processing.

(b) Each of the following processing activities presents significant risk to consumers' privacy:

(1) Selling or sharing personal information.

(2) Processing sensitive personal information.

(A) A business that processes the sensitive personal information of its employees or independent contractors solely and specifically for purposes of administering compensation payments, determining and storing employment authorization, administering employment benefits, or wage reporting as required by law, is not required to conduct a risk assessment for the processing of sensitive personal information for these purposes. Any other processing of consumers' sensitive personal information is subject to the risk-assessment requirements set forth in this Article.

(3) Using automated decisionmaking technology for a significant decision concerning a consumer or for extensive profiling.

(A) For purposes of this Article, "significant decision" means a decision using information that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5), that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).

(i) Education enrollment or opportunity includes:

1. Admission or acceptance into academic or vocational programs;

2. Educational credentials (e.g., a degree, diploma, or certificate); and

3. Suspension and expulsion.

(ii) Employment or independent contracting opportunity or compensation includes:

1. Hiring;

2. Allocation or assignment of work; salary, hourly or per-assignment compensation, incentive compensation such as a bonus, or another benefit ("allocation/assignment of work and compensation");

3. Promotion; and

4. Demotion, suspension, and termination.

(B) For purposes of this Article, "extensive profiling" means:

(i) Profiling a consumer through systematic observation when they are acting in their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor ("work or educational profiling");

(ii) Profiling a consumer through systematic observation of a publicly accessible place ("public profiling"); or

(iii) Profiling a consumer for behavioral advertising.

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

(A) For a significant decision concerning a consumer;

(B) To establish individual identity;

(C) For physical or biological identification or profiling;

(D) For the generation of a deepfake; or

(E) For the operation of generative models, such as large language models.

(c) Illustrative examples of when a business must conduct a risk assessment:

(1) Business A is a rideshare provider. Business A seeks to use automated decisionmaking technology to allocate rides and determine fares and bonuses for its drivers. Business A must conduct a risk assessment because it seeks to use automated decisionmaking technology for a significant decision concerning a consumer.

(2) Business B is hiring a new employee. Business B seeks to use emotion-assessment technology as part of the job interview process to determine who to hire. Business B must conduct a risk assessment because it seeks to use automated decisionmaking

technology (specifically, physical or biological identification or profiling) for a significant decision concerning a consumer.

(3) Business C provides a mobile dating application. Business C seeks to disclose consumers' precise geolocation and the ethnicity and medical information the consumers provided in their dating profiles to Business C's analytics service provider. Business C must conduct a risk assessment because it seeks to process sensitive personal information of consumers.

(4) Business D provides a personal-budgeting application into which consumers enter their financial information, including income. Business D seeks to display advertisements to these consumers on different websites for payday loans that are based on evaluations of these consumers' personal preferences, interests, and reliability. Business D must conduct a risk assessment because it seeks to conduct extensive profiling and share personal information.

(5) Business E is a grocery store chain. Business E seeks to process consumers' device media access control (MAC) addresses via Wi-Fi tracking to observe consumers' shopping patterns within its grocery stores. Business E must conduct a risk assessment because it seeks to profile consumers through systematic observation of a publicly accessible place.

(6) Business F is a technology provider. Business F seeks to extract faceprints from consumers' photographs to train Business F's facial-recognition technology. Business F must conduct a risk assessment because it seeks to process consumers' personal information to train automated decisionmaking technology or artificial intelligence that is capable of being used to establish individual identity.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7151. Stakeholder Involvement for Risk Assessments.

(a) The business must ensure that relevant individuals prepare, contribute to, or review the risk assessment, based upon their level of involvement in the processing activity that is subject to the risk assessment. Relevant individuals are those whose job duties pertain to the processing activity. For example, relevant individuals may be part of the business's product, fraud-prevention, or compliance teams. These individuals must make good faith efforts to disclose all facts necessary to conduct the risk assessment and must not misrepresent in any manner any fact necessary to conduct the risk assessment.

(b) A risk assessment may involve external parties to identify, assess, and mitigate the risks to consumers' privacy. These external parties may include, for example, service providers, contractors, experts in detecting and mitigating bias in automated decisionmaking technology, a subset of the consumers whose personal information the business seeks to process, or stakeholders that represent consumers' or others' interests, including consumer advocacy organizations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code. **§ 7152. Risk Assessment Requirements.**

(a) The business must conduct a risk assessment to determine whether the risks to consumers' privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing. The business must conduct and document the risk assessment as set forth below:

(1) The business must specifically identify its purpose for processing consumers' personal information. The purpose must not be identified or described in generic terms, such as "to improve our services" or for "security purposes."

(2) The business must identify the categories of personal information to be processed and whether they include sensitive personal information. This must include:

(A) The minimum personal information that is necessary to achieve the purpose of processing consumers' personal information.

(B) For uses of automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsections (b)(3)–(4), the business must identify the actions the business has taken or any actions it plans to take to maintain the quality of personal information processed by the automated decisionmaking technology or artificial intelligence.

(i) "Quality of personal information" includes completeness, representativeness, timeliness, validity, accuracy, consistency; and reliability of the sources of the personal information for the business's proposed use of the automated decisionmaking technology or artificial intelligence.

(ii) Actions a business may take to ensure quality of personal information include: (1) identifying the source of the personal information and whether that source is reliable (or, if known, whether the original source of the personal information is reliable); (2) 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 automated decisionmaking technology or artificial intelligence; (3) identifying whether the personal information contains sufficient breadth to address the range of real-world inputs the automated decisionmaking technology or artificial intelligence may encounter; and (4) identifying how errors from data entry, machine processing, or other sources are measured and limited.

(3) The business must identify the following operational elements of its processing:

(A) The business's planned method for collecting, using, disclosing, retaining, or otherwise processing personal information, and the sources of the personal information.

(B) How long the business will retain each category of personal information, and any criteria used to determine that retention period.

(C) The relationship between the consumer and the business, including whether the consumer interacts with the business, how they do so (e.g., via websites, applications, or offline), and the nature of the interaction (e.g., to obtain a good or service from the business).

(D) The approximate number of consumers whose personal information the business seeks to process.

(E) What disclosures the business has made or plans to make to the consumer about the processing, how these disclosures were made (e.g., via a just-in-time notice), and what actions the business has taken or plans to take to make these disclosures specific, explicit, prominent, and clear to the consumer.

(F) The names or categories of the service providers, contractors, or third parties to whom the business discloses or makes available the consumers' personal information for the processing; the purpose for which the business discloses or makes the consumers' personal information available to them; and what actions the business has taken or plans to take to make consumers aware of the involvement of these entities in the processing.

(G) The technology to be used in the processing. For the uses of automated decisionmaking technology set forth in section 7150, subsections (b)(3), the business must identify:

(i) The logic of the automated decisionmaking technology, including any assumptions or limitations of the logic; and

(ii) The output of the automated decisionmaking technology, and how the business will use the output.

(4) The business must specifically identify the benefits to the business, the consumer, other stakeholders, and the public from the processing of the personal information. For example, a business must not identify a benefit as "improving our service," because this does not identify the specific improvements to the service nor how the benefit resulted from the processing. If the benefit resulting from the processing is that the business profits monetarily (e.g., from the sale or sharing of consumers' personal information), the business must identify this benefit and, when possible, estimate the expected profit.

(5) The business must specifically identify the negative impacts to consumers' privacy associated with the processing. The business must identify the sources and causes of these negative impacts, and any criteria that the business used to make these determinations.

Negative impacts to consumers' privacy that a business may consider include the following:

(A) Unauthorized access, destruction, use, modification, or disclosure of personal information; and unauthorized activity resulting in the loss of availability of personal information.

(B) Discrimination upon the basis of protected classes that would violate federal or state antidiscrimination law.

(C) Impairing consumers' control over their personal information, such as by providing insufficient information for consumers to make an informed decision regarding the processing of their personal information, or by interfering with consumers' ability to make choices consistent with their reasonable expectations.

(D) Coercing or compelling consumers into allowing the processing of their personal information, such as by conditioning consumers' acquisition or use of an online service upon their disclosure of personal information that is unnecessary to the expected functionality of the service, or requiring consumers to consent to processing when such consent cannot be freely given.

(E) Disclosing a consumer's media consumption (e.g., books they have read or videos they have watched) in a manner that chills or deters their speech, expression, or exploration of ideas.

(F) Economic harms, including limiting or depriving consumers of economic opportunities; charging consumers higher prices; compensating consumers at lower rates; or imposing additional costs upon consumers, including costs associated with the unauthorized access to consumers' personal information.

(G) Physical harms to consumers or to property, including processing that creates the opportunity for physical or sexual violence.

(H) Reputational harms, including stigmatization, that would negatively impact an average consumer. Examples of processing activities that result in such harms include a mobile dating application's disclosure of a consumer's sexual or other preferences in a partner; a business stating or implying that a consumer has committed a crime without verifying this information; or a business processing consumers' biometric information to create a deepfake of them.

(I) Psychological harms, including emotional distress, stress, anxiety, embarrassment, fear, frustration, shame, and feelings of violation, that would negatively impact an average consumer. Examples of such harms include emotional distress resulting from disclosure of nonconsensual intimate imagery; stress and anxiety from regularly targeting a consumer who visits websites for substance abuse resources with advertisements for alcohol; or emotional distress from disclosing a consumer's purchase of pregnancy tests or emergency contraception for non-medical purposes.

(6) The business must identify the safeguards that it plans to implement to address the negative impacts identified in subsection (a)(5). The business must specifically identify how these safeguards address the negative impacts identified in subsection (a)(5), including to what extent they eliminate or reduce the negative impacts; and identify any safeguards the business will implement to maintain knowledge of emergent risks and countermeasures.

(A) Safeguards that a business may consider include the following:

(i) Encryption, segmentation of information systems, physical and logical access controls, change management, network monitoring and defenses, and data and integrity monitoring;

(ii) Use of privacy-enhancing technologies, such as trusted execution environments, federated learning, homomorphic encryption, and differential privacy;

(iii) Consulting external parties, such as those described in section 7151, subsection (b), to ensure that the business maintains current knowledge of emergent privacy risks and countermeasures; and using that knowledge to identify, assess, and mitigate risks to consumers' privacy; and

(iv) Evaluating the need for human involvement as part of the business's use of automated decisionmaking technology, and implementing policies, procedures, and training to address the degree and details of human involvement identified as necessary in that evaluation.

(B) For uses of automated decisionmaking technology set forth in section 7150, subsection (b)(3), the business must identify the following:

(i) Whether it evaluated the automated decisionmaking technology to ensure it works as intended for the business's proposed use and does not discriminate based upon protected classes ("evaluation of the automated decisionmaking technology"); and

(ii) The policies, procedures, and training the business has implemented or plans to implement to ensure that the automated decisionmaking technology works as intended for the business's proposed use and does not discriminate based upon protected classes ("accuracy and nondiscrimination safeguards"). For example, if a business determines that the use of low-quality enrollment images creates a high risk of false-positive matches in its proposed use of facial-recognition technology, the business must identify the policies, procedures, and training it has implemented or plans to implement to ensure that it is using only sufficiently high-quality enrollment images to mitigate that risk.

(iii) Where a business obtains the automated decisionmaking technology from another person, the business must identify the following:

1. Whether it reviewed that person's evaluation of the automated decisionmaking technology, and whether that person's evaluation included any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology.

2. Any accuracy and nondiscrimination safeguards that it implemented or plans to implement.

(7) The business must identify whether it will initiate the processing subject to the risk assessment.

(8) The business must identify the contributors to the risk assessment. In the risk assessment or in a separate document maintained by the business, the business must identify the individuals within the business and the external parties that contributed to the risk assessment.

(9) The business must identify the date the assessment was reviewed and approved, and the names and positions of the individuals responsible for the review and approval. The individuals responsible for the review and approval must include the individual who decides whether the business will initiate the processing that is subject to the risk assessment. If the business presented or summarized its risk assessment to the business's board of directors or governing body for review, or if no such board or equivalent body exists, to the business's highest-ranking executive who is responsible for oversight of risk-assessment compliance for review, the business must include the date of that review.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

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

(a) A business that makes automated decisionmaking technology or artificial intelligence available to another business ("recipient-business") for any processing activity set forth in section 7150, subsection (b), must provide all facts necessary to the recipient-business for the recipient-business to conduct its own risk assessment.

(b) A business that trains automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsection (b)(4) and permits another person to use that automated decisionmaking technology or artificial intelligence, must provide to the person a plain language explanation of any requirements or limitations that the business identified as relevant to the permitted use of automated decisionmaking technology or artificial intelligence.

(c) The requirements of this section apply only to automated decisionmaking technology and artificial intelligence trained using personal information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

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

(a) The business must not process personal information for any processing activity identified in section 7150, subsection (b), if the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public from the processing.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code. **§ 7155. Timing and Retention Requirements for Risk Assessments.**

(a) A business must comply with the following timing requirements for conducting and updating its risk assessments:

(1) A business must conduct and document a risk assessment in accordance with the requirements of this Article before initiating any processing activity identified in section 7150, subsection (b).

(2) At least once every three years, a business must review, and update as necessary, its risk assessments to ensure that they remain accurate in accordance with the requirements of this Article.

(3) Notwithstanding subsection (a)(2) of this section, a business must immediately update a risk assessment whenever there is a material change relating to the processing activity. A change relating to the processing activity is material if it diminishes the benefits of the processing activity as set forth in section 7152, subsection (a)(4), creates new negative impacts or increases the magnitude or likelihood of previously identified negative impacts as set forth in section 7152,

subsection (a)(5), or diminishes the effectiveness of the safeguards as set forth in section 7152, subsection (a)(6).

Material changes may include, for example, changes to the purpose of the processing; the minimum personal information necessary to achieve the purpose of the processing; or the risks to consumers' privacy raised by consumers (e.g., numerous consumers complain to a business about the risks that the business's processing poses to their privacy).

(b) A business must retain its risk assessments, including original and updated versions, for as long as the processing continues or for five years after the completion of the risk assessment, whichever is later.

(c) For any processing activity identified in section 7150, subsection (b), that the business initiated prior to the effective date of these regulations and that continues after the effective date of these regulations, the business must conduct and document a risk assessment in accordance with the requirements of this Article within 24 months of the effective date of these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

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

(a) A business may conduct a single risk assessment for a comparable set of processing activities. A "comparable set of processing activities" that can be addressed by a single risk assessment is a set of similar processing activities that present similar risks to consumers' privacy.

(1) For example, Business G sells toys to children and is considering using in-store paper forms to collect names, mailing addresses, and birthdays from children that visit their stores, and to use that information to mail a coupon and list of age-appropriate toys to each child during the child's birth month and every November. Business G uses the same service providers and technology for each category of mailings across all stores. Business G must conduct and document a risk assessment because it is processing sensitive personal information. Business G may use a single risk assessment for processing the personal information for the birthday mailing and November mailing across all stores because in each case it 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.

(b) If the business has conducted and documented a risk assessment for the purpose of complying with another law or regulation that meets all the requirements of this Article, the business is not required to conduct a duplicative risk assessment. If the risk assessment conducted and documented for the purpose of compliance with another law

or regulation does not meet all of the requirements of this Article, the business must supplement the risk assessment with any additional information required to meet all of the requirements of this Article.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7157. Submission of Risk Assessments to the Agency.

(a) Timing of Risk Assessment Submissions.

(1) First Submission. A business has 24 months from the effective date of these regulations to submit the risk assessment materials regarding the risk assessments that it has conducted from the effective date of these regulations to the date of submission ("first submission"). The risk assessment materials are set forth in subsection (b) and must be submitted to the Agency as set forth in subsection (c).

(2) Annual Submission. After the business completes its first submission to the Agency as set forth in subsection (a)(1), its subsequent risk assessment materials must be submitted every calendar year to the Agency, and there must be no gap in the months covered by successive submissions of risk assessment materials ("subsequent annual submissions").

(b) Risk Assessment Materials to Be Submitted. The first submission and subsequent annual submissions of the risk assessment materials to the Agency must include the following:

(1) Certification of Conduct. The business must submit a written certification that the business conducted its risk assessment as set forth in this Article during the months covered by the first submission and subsequent annual submissions to the Agency on a form provided by the Agency.

(A) The business must designate a qualified individual with authority to certify the conduct of the risk assessment on behalf of the business. This individual must be the business's highest-ranking executive who is responsible for oversight of the business's risk-assessment compliance in accordance with this Article ("designated executive").

(B) The written certification must include:

(i) Identification of the months covered by the submission period for which the business is certifying its conduct of the risk assessment and the number of risk assessments that the business conducted and documented during that submission period;

(ii) An attestation that the designated executive has reviewed, understood, and approved the business's risk assessments that were conducted and documented as set forth in this Article;

(iii) An attestation that the business initiated any of the processing set forth in section 7150, subsection (b), only after the business conducted and documented a risk assessment as set forth in this Article; and

(iv) The designated executive's name, title, and signature, and the date of certification.

(2) Risk Assessments in Abridged Form. For each risk assessment conducted and documented or updated by the business during the submission period, the business must submit an abridged version of the new or updated risk assessment to the Agency on a form provided by the Agency that includes:

(A) Identification of the processing activity in section 7150, subsection (b), that triggered the risk assessment;

(B) A plain language explanation of its purpose for processing consumers' personal information;

(C) The categories of personal information processed, and whether they include sensitive personal information; and

(D) A plain language explanation of the safeguards that the business has implemented or plans to implement as set forth in section 7152, subsection (a)(6). A business is not required to provide information that would compromise its ability to prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information; resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or ensure the physical safety of natural persons.

(3) Risk Assessments in Unabridged Form. A business also may include in its submission to the Agency a hyperlink that, if clicked, will lead to a public webpage that contains its unabridged risk assessment.

(4) Exemptions.

(A) A business is not required to submit a risk assessment to the Agency if the business does not initiate the processing activity subject to the risk assessment.

(B) If a business previously conducted a risk assessment for a processing activity in compliance with this Article and submitted an abridged risk assessment to the Agency, and there were no material changes to that processing during a subsequent submission period, the business is not required to submit an updated risk assessment to the Agency. The business must still submit a certification of the conduct of its risk assessment to the Agency.

(c) Method of Submission. The risk assessment materials must be submitted to the Agency through the Agency's website at https://cppa.ca.gov/.

(d) Risk Assessments Must Be Provided to the Agency or to the Attorney General Upon Request. The Agency or the Attorney General may require a business to provide its unabridged risk assessments to the Agency or to the Attorney General at any time. A business must provide its unabridged risk assessments within 10 business days of the Agency's or the Attorney General's request.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.