

## Version 3 Proposed Draft Amendments to the CPA Rules (12-05-24)

Version 1, Draft Amendments to the CPA Rules (9/25/2024) in red with a single underline.  
Version 2, Draft Amendments to the CPA Rules for hearing (10/30/2024) in blue with a double underline.  
Version 3, Draft Amendments to the CPA Rules based on written comments and public testimony received through 11/7/2024 (12/05/24) in green with a dotted underline.

### COLORADO DEPARTMENT OF LAW

#### Consumer Protection Section

#### Colorado Privacy Act Rules

#### 4 CCR 904-3

##### PART 1 GENERAL APPLICABILITY

##### Rule 1.01 BASIS, SPECIFIC STATUTORY AUTHORITY, AND PURPOSE

The rules in this Part 904-3 are developed pursuant to C.R.S. § 6-1-108(1), which grants the Attorney General the authority to promulgate such rules as may be necessary to administer the provisions of the Colorado Consumer Protection Act, and to C.R.S. § 6-1-1313, which: (1) gives the Attorney General authority to promulgate ~~R~~rules for the purpose of carrying out the Colorado Privacy Act; (2) requires the Attorney General to adopt ~~R~~rules that detail the technical specifications for one or more Universal Opt-Out Mechanisms that clearly communicate a Consumer's affirmative, freely given, and unambiguous choice to opt out of the Processing of Personal Data for purposes of Targeted Advertising or the Sale of Personal Data pursuant to C.R.S. §§ 6-1-1306(1)(a)(I)(A) or (1)(a)(I)(B); ~~;~~ and (3) gives the Attorney General the authority to adopt rules that govern the process of issuing opinion letters and interpretive guidance to develop an operational framework for business that includes a good faith reliance defense of an action that may otherwise constitute a violation of Part 13. Effective July 1, 2025, these rules are also developed pursuant to C.R.S. § 6-1-1314(7), which gives the Colorado Department of Law the authority to promulgate rules for the implementation of C.R.S. § 6-1-1314.

These rules are promulgated to establish implementation and operational guidelines for the Colorado Privacy Act, and to help ensure that the Colorado Privacy Act is carried out in a way that is consistent with the intent of the General Assembly, as reflected in the legislative declaration at C.R.S. § 6-1-1302.

\*\*\*\*\*

##### Rule 1.03 EFFECTIVE DATE

Except for the provisions that have delayed effective dates as stated in these rules or C.R.S. §§ 6-1-1301 through 6-1-1314~~43-et seq.~~, these rules shall become effective July 1, 2023- by the effective date published by the Secretary of State in the Colorado Code of Regulations.

\*\*\*\*\*

##### PART 2 DEFINITIONS

##### Rule 2.01 AUTHORITY AND PURPOSE

- A. The statutory authority for the rules in this Part 2 is C.R.S. §§ 6-1-108(1), 6-1-1303, and 6-1-1313. The purpose of these rules is to define certain undefined terms that are used throughout the Colorado Privacy Act, C.R.S. §§ 6-1-1301, ~~et seq. through 6-1-1314~~, and these Colorado Privacy Act Rules, 4 CCR 904-3, including but not limited to certain undefined terms that are used in the definitions set forth in C.R.S. § 6-1-1303. The terms defined by this rule and C.R.S. § 6-1-1303 are capitalized where they appear in the rules to let the reader know to refer back to the

definitions. When a term is used in a conventional sense, and is not intended to be a defined term, it is not capitalized.

Rule 2.02      DEFINED TERMS

The following definitions of terms, in addition to those set forth in C.R.S. § 6-1-1303, apply to these Colorado Privacy Act Rules, 4 CCR 904-3, promulgated pursuant to the Colorado Privacy Act, unless the context requires otherwise:

\*\*\*\*\*

**“Biometric Data”** ~~is defined as set forth in as referred to in~~ C.R.S. § 6-1-1303(2.24)(b), and means one or more Biometric Identifiers that are used or intended to be used, singly or in combination with each other or with other Personal Data, for identification purposes. Unless such data is used for identification purposes, “Biometric Data” does not include the following unless the Biometric Data is used for identification purposes: (a) a digital or physical photograph; (b) an audio or voice recording; or (c) any data generated from a digital or physical photograph or an audio or video recording.

**“Biometric Identifiers”** ~~is defined as set forth in C.R.S. § 6-1-1303(2.4), and~~ means data generated by the technological processing, measurement, or analysis of an individual’s biological, physical, or behavioral characteristics, which data that can be Processed for the purpose of uniquely identifying an individual. Biometric Identifier includes, including but not limited to a fingerprint; a voiceprint; a scans or records of eye retinas or irises; a facial mapping, facial geometry, or facial templates; or other unique biological, physical, or behavioral patterns or characteristics.

**“Biometric Identifier Notice”** means the notice of collection or processing of Biometric Identifiers containing the disclosures required by C.R.S. § 6-1-1314(4)(a).

\*\*\*\*\*

**“Child”** is defined as set forth in C.R.S. § 6-1-1303(4), and means an individual under thirteen years of age.

\*\*\*\*\*

**“Data Right”** or **“Data Rights”** means the Consumer Personal Data rights granted in C.R.S. §§ 6-1-1306(1) and 6-1-1314(5).

\*\*\*\*\*

**“Employee”** except as used in C.R.S. § 6-1-1314, means any person, acting as a job applicant to, or performing labor or services for the benefit of an Employer, including contingent and temporary workers and migratory laborers.

**“Employee”** as used in C.R.S. § 6-1-1314 is set forth in C.R.S. § 6-1-1314(1)(b) and means an individual who is employed full-time, part-time, or on-call or who is hired as a contractor, subcontractor, intern, or fellow.

\*\*\*\*\*

**“Interpretive Guidance”** means a written statement issued by the Attorney General that calls attention to a well-established interpretation or principle of the Colorado Privacy Act or any rules or regulations promulgated thereunder, without applying it to a specific factual situation.

\*\*\*\*\*

“Minor” is defined as set forth in C.R.S. § 6-1-1303 (16.5) and means any consumer who is under eighteen years of age.

\*\*\*\*\*

“Opinion Letter” means a letter containing the Attorney General’s opinion as to the application of one or more sections of the Colorado Privacy Act, C.R.S. § 6-1-1301, et seq., and any rules or regulations promulgated thereunder, to a specific factual situation.

\*\*\*\*\*

## PART 3 CONSUMER DISCLOSURES

### Rule 3.01 AUTHORITY AND PURPOSE

- A. The statutory authority for the rules in this Part 3 is C.R.S. §§ 6-1-108(1), ~~and 6-1-1313, and 6-1-1314.~~ The purpose of the rules in Part 3 is to ensure that disclosures, notifications, and other communications to Consumers are clear, accessible, and understandable to Consumers so that Consumers can understand and exercise the full scope of their rights under the Colorado Privacy Act, C.R.S. § 6-1-1303 ~~through 6-1-1314~~ et seq.

### Rule 3.02 REQUIREMENTS FOR DISCLOSURES, NOTIFICATIONS, AND OTHER COMMUNICATIONS TO CONSUMERS

- A. Disclosures, notifications, and other communications to Consumers pursuant to 4 CCR 904-3, Rules 4.02, 4.05(D), 5.03, 6.02, 6.05, and 7.04 must be:
1. Designed to be understandable and accessible to a Controller’s target audiences, considering the vulnerabilities or unique characteristics of the audience and paying particular attention to the vulnerabilities of ~~Ce~~children or Minors. For example, they shall use plain, straightforward language and avoid technical or legal jargon.

\*\*\*\*\*

- B. A written Biometric Data policy required by C.R.S. § 6-1-1314(2)(a) shall comply with all requirements for disclosures and communications to Consumers provided in 4 CCR 904-3, Rule 3.02(A).

## PART 4 CONSUMER PERSONAL DATA RIGHTS

### Rule 4.01 AUTHORITY AND PURPOSE

- A. The statutory authority for the rules in this Part 4 is C.R.S. §§ 6-1-108(1), 6-1-1306, ~~and 6-1-1313, and 6-1-1314.~~ The purpose of the rules in Part 4 is to clarify the scope of Consumer Personal Data rights, and standards for the processes required to facilitate the exercise of those rights.

\*\*\*\*\*

### Rule 4.04 RIGHT OF ACCESS

\*\*\*\*\*

- B. If a Consumer right to access includes Biometric Data, the Controller must also include the additional information required at C.R.S. § 6-1-1314(5).
-

- C. Personal Data provided in response to an access request must:
1. Be provided in a form that is concise, transparent and easily intelligible and in an appropriate, commonly used electronic format, depending on the nature of the data;
  2. Be available in the language in which the Consumer interacts with the Controller.
  3. Avoid incomprehensible internal codes and, if necessary, include explanations that would allow the average Consumer to make an informed decision of whether to exercise deletion, correction, or opt-out rights.
  4. Be provided in compliance with the requirements for disclosures, notifications, and other communications, as described in 4 CCR 904-3, Rule 3.02, as applicable.
- DE. The Controller shall implement and maintain reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, in Processing any documentation relating to a Consumer's access request.
- ED. A Controller shall not be required to disclose in response to an access request a Consumer's government-issued identification number, financial account number, health insurance or medical identification number, an account password, security questions and answers, Biometric Data, or Biometric Identifiers. The Controller shall, however, inform the Consumer with sufficient particularity that it has collected that type of information. For example, a Controller shall respond that it collects "unique Biometric Data including a fingerprint scan" without disclosing the actual fingerprint scan data.
- FE. If a Consumer exercises the right to access their Personal Data in a portable format pursuant to C.R.S. § 6-1-1306(1)(e) and the Controller determines the manner of response would reveal the Controller's trade secrets, the Controller must still honor the Consumer's undiminished right of access in a format or manner which would not reveal trade secrets, such as in a nonportable format.

\*\*\*\*\*

## PART 6 DUTIES OF CONTROLLERS

### Rule 6.01 AUTHORITY AND PURPOSE

- A. The statutory authority for the rules in this Part 6 is C.R.S. §§ 6-1-108(1), 6-1-1308, ~~and 6-1-1313~~, and 6-1-1314. The purpose of the rules in this Part 6 is to provide clarity on the duties of Controllers concerning the Personal Data of Colorado Consumers.

\*\*\*\*\*

### Rule 6.12 BIOMETRIC IDENTIFIER NOTICE

- A. Controllers required to provide a Biometric Identifier Notice shall comply with all requirements for disclosures and communications to Consumers provided in 4 CCR 904-3, Rule 3.02.
- B. The Biometric Identifier Notice shall occur at or before the ~~initial~~ collection or Processing of any Biometric Identifiers, or before a material change to the Processing purpose of a Biometric Identifier.
- C. A Biometric Identifier Notice must be clear. Information contained in such notice shall be:

1. Concrete and definitive, avoiding abstract or ambivalent terms that may lead to varying interpretations.
  2. If included in a privacy notice, clearly labeled, such that Consumers seeking to understand a Controller's collection and use of Biometric Identifiers can easily access the section of the privacy notice containing relevant information.
- D. A Biometric Identifier Notice must be reasonably accessible. Such notice may be:
1. A separate notice, or included within a general privacy notice if the privacy notice is clearly labeled as required by 4 CCR 904-3, Rule 6.12(C)(2); and made available in its entirety prior to the collection or Processing of Biometric Identifiers; or
  2. Made available in its entirety prior to the collection or Processing of Biometric Identifiers, or linked from a website's homepage, and if applicable, a mobile application's app store page or download page.
    - a. Linked to from A link made available on the homepage of a website or on a mobile application's app store page or download page. If using a link, the link must be conspicuous and must clearly indicate it relates to Biometric Identifiers in the link text. A Controller that Processes Biometric Identifiers and maintains an application on a mobile or other device shall also include a link to the Biometric Identifier Notice in the application's settings menu.
    - b. If the link directs to a privacy notice, it must point the Consumer to the specific section of the privacy notice that includes the Biometric Identifier Notice disclosures.
- E. A Controller that does not operate a website shall make the Biometric Identifier Notice conspicuously available to Consumers through a medium regularly used by the Controller to interact with Consumers. For instance, if a Controller interacts with a Consumer offline, an offline version of the privacy notice must be available to the Consumer.

\*\*\*\*\*

## PART 7 CONSENT

### Rule 7.01 AUTHORITY AND PURPOSE

- A. The statutory authority for the rules in this Part 7 is C.R.S. §§ 6-1-108(1), 6-1-1303(5), 6-1-1306, 6-1-1308, 6-1-1308.5 (eff. Oct. 1, 2025), and 6-1-1313–and 6-1-1314(4) (eff. July 1, 2025). The purpose of the rules in this Part 7 is to provide clarity on the requirements to obtain Consent when Consent is required under the statute, including the prohibition against obtaining agreement through the use of Dark Patterns.

### Rule 7.02 REQUIRED CONSENT

- A. Pursuant to C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7), and 6-1-1308.5, and 6-1-1314(4) a Controller must obtain valid Consumer Consent prior to:
1. Processing a Consumer's Sensitive Data;
  2. Processing Personal Data concerning a known Child, in which case the Child's parent or lawful guardian must provide Consent;

3. Selling a Consumer's Personal Data, Processing a Consumer's Personal Data for Targeted Advertising, or Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer after the Consumer has exercised the right to opt out of the Processing for those purposes; ~~and~~
4. Processing Personal Data for purposes that are not reasonably necessary to, or compatible with, the original specified purposes for which the Personal Data are Processed;
5. Processing the Personal Data of a Consumer whom the Controller actually knows or willfully disregards is a Minor as contemplated in C.R.S. § 6-1-1308.5(2);
6. Using any system design feature to significantly increase, sustain, or extend the a Minor's use of an online service, product, or feature by a Consumer whom the Controller actually knows or willfully disregards is a Minor, as contemplated in C.R.S § 6-1-1308.5(2); and
7. Selling, leasing, trading, disclosing, redisclosing, or otherwise disseminating Biometric Identifiers, subject to the exceptions in 6-1-1314(4)(b).

\*\*\*\*\*

Rule 7.08 REFRESHING CONSENT

- A. When a Consumer has not interacted with a Controller in the prior twenty-four (24) months, the Controller must refresh Consent in compliance with all requirements of this Part 7 to:
    1. Continue Processing Sensitive Data pursuant to C.R.S. § 6-1-1308(7); or
    2. Continue Processing Personal Data for a Secondary Use pursuant to C.R.S. § 13-8(4), if the Secondary Use involves Profiling for a decisions that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.
  - B. Controllers are not required to refresh Consent under part A of this section where a Consumer has access and ability to update their opt-out preferences at any time through a user-controlled interface.
  - C. If a Processing purpose materially evolves such that the new purpose becomes a secondary use pursuant to C.R.S. § 6-1-1308(4), the Consumer's original Consent is no longer valid, and the Controller must obtain new Consent pursuant to Part 7 of these rules.
  - D. Employers required to obtain Consent pursuant to C.R.S. § 6-1-1314(6)(b) are not required to refresh Consent under part A of this section.
    1. Employers required to obtain Consent pursuant to C.R.S. § 6-1-1314(6)(b) must refresh Consent in compliance with all requirements of this Part 7 when:
      - a. Processing additional categories of an Employee's Biometric Identifier for which the Employee has not yet provided consent; and
      - b. Processing an Employee's Biometric Identifier for a Secondary Use.
-

2. To comply with C.R.S. § 6-1-1314(6)(b), Consent must be obtained from an Employee. Consent obtained from a prospective Employee during the hiring process is not sufficient to fulfill the requirements of C.R.S. § 6-1-1314(6)(b).

Rule 7.09 EMPLOYEE CONSENT TO COLLECT AND PROCESS BIOMETRIC IDENTIFIERS

- A. Employers may only require as a condition of employment that an Employee or a prospective Employee Consent to the collection and Processing of the Employee's or prospective Employee's Biometric Identifier consistent with C.R.S. § 6-1-1314(6).
- B. Consent requested by an Employer to collect or Process an Employee's or prospective Employee's Biometric Identifier shall be consistent with all requirements for disclosures and communications to Consumers provided in 4 CCR 904-3, Rule 3.02(A).
- C. Consent required by an Employer to collect or process an Employee's or prospective Employee's Biometric Identifier shall be consistent with the requirements for Consent provided in 4 CCR 904-3, Rules 7.03-7.08:

Rule 7.~~09~~10 USER INTERFACE DESIGN, CHOICE ARCHITECTURE, AND DARK PATTERNS

\*\*\*\*\*

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, 6-1-1309.5, and 6-1-1313. 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 or to a Minor, pursuant to C.R.S. § 6-1-1309(3), and C.R.S. § 6-1-1309.5, 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; and 5) fulfills any additional obligations as required by C.R.S. § 6-1-1309.5.

\*\*\*\*\*

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 Personal Data from a Minor if required by C.R.S. § 6-1-1309.5 as described in C.R.S. § 6-1-1303(16.5); or Sensitive Data, including Personal Data from a known Child as described in C.R.S. § 6-1-1303(24);

\*\*\*\*\*

6. The sources and nature of risks to the rights of Consumers associated with the Processing activity posed by the Processing activity-, including the sources and nature of any heightened risk of harm to Minors that is a reasonable foreseeable result of offering an online service, product, or feature to Minors. 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; or
  - 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.

\*\*\*\*\*

Rule 8.05      TIMING

\*\*\*\*\*

- F. Unless otherwise specified, dD Data protection assessments shall be required for activities created or generated after July 1, 2023. This requirement is not retroactive.
- G. Data protection assessments conducted pursuant to C.R.S. § 6-1-1309.5 shall be required for activities created or generated after October 1, 2025. This requirement is not retroactive.
-



\*\*\*\*\*

**PART 10 INTERPRETIVE GUIDANCE AND OPINION LETTERS**

**Rule 10.01 AUTHORITY AND PURPOSE**

- A. The statutory authority for the rules in this Part 10 is C.R.S. § 6-1-1313. The purpose of the rules in Part 10 is to create a process of issuing Opinion Letters to develop an operational framework for businesses that includes a good faith reliance defense, and to create a process of issuing statements of interpretive guidance to provide guidance to covered individuals and the general public.

**Rule 10.02 SCOPE AND EFFECT OF OPINION LETTERS**

- A. Opinion Letters are only issued in response to requests made pursuant to 4 CCR 904-3, Rule 10.043.
- B. Opinion letters will contain the Attorney General's opinion regarding the application of the Colorado Privacy Act to parties' proposed activities, as described in requests made pursuant to 4 CCR 904-3, Rule 10.04.
- C. The Attorney General shall determine, at the Attorney General's discretion, whether to issue an Opinion Letter. In making this determination, the Attorney General may consider factors including, without limitation, whether:
1. The Opinion Letter will terminate a controversy or remove one or more uncertainties as to the application of the law to the requestor's situation;
  2. The request involves a subject, question, or issue that concerns a formal or informal matter or investigation currently pending before the secretary or a court; and
  3. The request seeks a ruling on a moot or hypothetical question.
- D. Should the Department of Law file an enforcement action against a person or entity regarding the question presented in an Opinion Letter, the person or entity who is the subject of that Opinion Letter may legally rely upon the Opinion Letter in asserting a good faith reliance defense.
1. The Attorney General will not normally investigate the underlying facts of the requestor's situation and, as a result, an Opinion Letter may not be applicable to the requestor if the request for opinion does not contain all material facts and representations, or if the underlying facts of the requestor's situation do not conform to the summary of material facts.
- E. Except as otherwise provided in an Opinion Letter in the Attorney General's sole determination, An Opinion Letter may not form the basis of a good faith reliance defense for persons or entities who were not the subject of that Opinion Letter as described in the Opinion Letter request.
- F. The scope and terms of an Opinion Letter will be set out in the Opinion Letter itself and may deviate from the interpretation proposed by the requestor in its submission.
- G. The Attorney General may decline any request to issue an Opinion Letter. The Attorney General may, when it is deemed appropriate, issue Interpretive Guidance calling attention to established principles under the Colorado Privacy Act, even when a request that was submitted was for an Opinion Letter.
-

Rule 10.03      REQUESTS FOR OPINION LETTERS

- A.      A request for an Opinion Letter must be prospective in nature, pertaining to an activity that the requestor in good faith specifically plans to undertake. The plans may be contingent upon receiving a favorable Opinion Letter.
- B.      Requests presenting a general question of interpretation, positing a hypothetical situation, or regarding the activities of unrelated Persons or entities do not qualify as Opinion Letter requests.
- C.      A request for an Opinion Letter may only be submitted by a Person or entity that will be directly affected by the activity that is the subject of the request.
- D.      A request for an opinion letter must be submitted in writing using the process specified on the Attorney General's website.
- E.      Each request for an Opinion Letter must be fact-specific and narrowly framed to the specific activity in question, and must set forth the facts underlying the request in as much detail as possible, including without limitation:
  - 1.      The name, title, address, and daytime telephone number of a contact person who will be available to discuss the request for an Opinion Letter with the Attorney General on behalf of the requestor.
  - 2.      The identities of the requestor and of all other actual and potential parties impacted by the activity that is subject to the request for an Opinion Letter.
  - 3.      A complete and specific description containing all relevant information bearing on the activity for which an Opinion Letter is requested, including without limitation:
    - a.      A complete and specific description of the activity, transaction or agreement that the requestor plans to undertake, or any Personal Data Processing that that will result from the activity, agreement or transaction that the requestor plans to pursue.
    - b.      A description of the personal data involved, including whether the personal data is sensitive personal data, and the category of sensitive data;
    - c.      A description of each of the parties that would have access to the Personal Data involved;
    - d.      A description and draft of any disclosures relating the Personal Data involved that will be provided to consumers, and a description of the location and form in which the disclosure will be provided;
    - e.      A copy of any data protection assessment conducted in anticipation of the contemplated Processing activity, if required by C.R.S. § 6-1-1309. Data protection assessments required by C.R.S. § 6-1-1309 are confidential and exempt from public inspection and copying under the Colorado Open records Data (CORA) Part 2 of Article 72 of Title 24. The disclosure of a data protection assessment in a request for an Opinion Letter does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information contained in the assessment; and

- f. If applicable, a designation of trade secrets or confidential commercial or financial information. Such information will be protected to the extent permitted by CORA, Part 2 of Article 72 of Title 24.
- F. The Attorney General may request additional information and documents from a person submitting a request for an Opinion Letter.
- G. A request for an Opinion Letter is complete when the Attorney General has determined that no additional information is necessary to consider the request.
- H. A request may be dismissed for failure to provide information requested by the Attorney General..

Rule 10.04 ISSUANCE OF OPINION LETTERS

- A. The Attorney General shall publish each issued Opinion Letter on the Attorney General's Website after an opinion is issued. The published form of each Opinion Letter shall redact and protect information required by CORA, Part 2 of Article 72 of Title 24, identifying information. However, Opinion Letters may contain information provided by the requesting party and sufficient facts to ascertain the identity of the requesting party.

Rule 10.05 SCOPE AND EFFECT OF INTERPRETIVE GUIDANCE

- A. The Attorney General may, in its discretion, issue statements providing Interpretive Guidance to covered individuals and the general public where the nature of a request from an individual or organization suggests that it is seeking general information, where a request from an individual or organization does not meet all the requirements of 4 CCR 904-3, Rule 10.04 of these Rules, or when the Attorney General believes that such general information will assist an individual, organization, or the general public.
- B. Interpretive Guidance issued by the Attorney General is informational only and is not binding on the Attorney General or Colorado Department of Law with respect to any particular factual situation.
- C. Interpretive Guidance issued pursuant to this section is for informational purposes only, and may not serve as the basis for a good faith reliance defense.
- D. Interpretive Guidance shall be published on the Attorney General website.

Rule 10.06 REQUESTS FOR INTERPRETIVE GUIDANCE

- A. Any Person affected directly or indirectly by the Colorado Privacy Act may request Interpretive Guidance from the Attorney General.
- B. The Attorney General may, when it is deemed appropriate, issue Interpretive Guidance calling attention to principles under the Colorado Privacy Act, even when a request that was submitted was for an Opinion Letter. The Attorney General may issue Interpretive Guidance regarding the Colorado Privacy Act, C.R.S. the Colorado Privacy Act, C.R.S. § 6-1-1303 through 6-1-1314, sua sponte.

PART 1~~10~~ ENFORCEMENT

Rule 1~~10~~.01 AUTHORITY AND PURPOSE

- A. The statutory authority for the rules in this Part 1~~10~~ is C.R.S. §§ 6-1-1310 and 6-1-1311. The purpose of the rules in this Part 10 is to clarify enforcement considerations related to the
-

Colorado Privacy Act, C.R.S. § 6-1-1303, ~~et seq. through 6-1-1314~~, and these Colorado Privacy Act Rules, 4 CCR 904-3.

Rule ~~119~~.02      ENFORCEMENT CONSIDERATIONS

- A.      Nothing in the Colorado Privacy Act, C.R.S. § 6-1-1303, ~~et seq. through 6-1-1314~~, or these Colorado Privacy Act Rules, 4 CCR 904-3, provides the Colorado Attorney General or District Attorney, as applicable, with enforcement powers that would infringe upon rights protected by the United States Constitution or Colorado Constitution, including the right to freedom of speech or freedom of the press.

PART ~~142~~      MATERIALS INCORPORATED BY REFERENCE

Rule ~~142~~.01      AUTHORITY AND PURPOSE

- A.      The statutory authority for the rules in this Part ~~142~~ is C.R.S. §§ 6-1-108(1) and 6-1-1313. The purpose of the rules in this Part ~~142~~ is to incorporate by reference the guidelines that are referred to in 4 CCR 904-3, Rule 3.02(A)(2).

Rule ~~142~~.02      WEB CONTENT ACCESSIBILITY GUIDELINES

\*\*\*\*\*