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 gives the Attorney General authority to promulgate Rules for the purpose of carrying out the Colorado Privacy Act and requires the Attorney General to adopt 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).

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 1.02 SEVERABILITY

If any provision of these Colorado Privacy Act Rules, 4 CCR 904-3, is found to be invalid by a court of competent jurisdiction, the remaining provisions of these rules shall remain in full force and effect.

Rule 1.03 EFFECTIVE DATE

Except for the provisions that have delayed effective dates as stated in these rules or C.R.S. §§ 6-1-1313 *et seq.,* these rules shall become effective July 1, 2023.

Rule 1.04 EXEMPTIONS

These Colorado Privacy Act Rules, 4 CCR 904-3, are subject to the applicability requirements and exemptions provided in C.R.S. § 6-1-1304.

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*., 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:

"**Authorized Agent**" as referred to in C.R.S. § 6-1-1306(1)(a)(II) means a person or entity authorized by the Consumer to act on the Consumer's behalf.

"**Biometric Data**" as referred to in C.R.S. § 6-1-1303(24)(b) means 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 (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**" means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics that can be Processed for the purpose of uniquely identifying an individual, including but not limited to a fingerprint, a voiceprint, scans or records of eye retinas or irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics.

"**Bona Fide Loyalty Program**" as referred to in C.R.S. § 1-6-1308(1)(d) is defined as a loyalty, rewards, premium feature, discount, or club card program established for the genuine purpose of providing Bona Fide Loyalty Program Benefits to Consumers that voluntarily participate in that program, such that the primary purpose of Processing Personal Data through the program is solely to provide Bona Fide Loyalty Program Benefits to participating Consumers.

"**Bona Fide Loyalty Program Benefit**" is defined as an offer of superior price, rate, level, quality, or selection of goods or services provided to a Consumer through a Bona Fide Loyalty Program. Such benefits may be provided directly by a Controller or through a Bona Fide Loyalty Program Partner.

"**Bona Fide Loyalty Program Partner**" is defined as a Third Party that provides Bona Fide Loyalty Program Benefits to Consumers through a Controller's Bona Fide Loyalty Program, either alone or in partnership with the Controller.

"**Commercial product or service**" as referred to in C.R.S. § 6-1-1304(1)(a) means a product or service bought, sold, leased, joined, provided, subscribed to, or delivered in exchange for monetary or other valuable consideration in the course of a Controller's business, vocation, or occupation.

"**Controller**" is defined as set forth in C.R.S. § 6-1-1303(7), and means a person that, alone or jointly with others, determines the purposes for and means of Processing Personal Data.

"**Data Broker**" is defined as a Controller that knowingly collects and sells to Third Parties the Personal Data of a Consumer with whom the Controller does not have a direct relationship.

"**Data Right**" or "**Data Rights**" means the Consumer Personal Data rights granted in C.R.S. § 6-1-1306(1).

"**Disability**" or "**Disabilities**" has the same meaning as set forth in C.R.S. § 24-85-102(2.3).

"**Employee**" 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.

"**Employer**" means every person, entity, firm, partnership, association, corporation, migratory field labor contractor or crew leader, receiver, or other officer of court, and any agent or officer thereof, of the above-mentioned classes, employing any person.

"**Employment Records**" as referred to in C.R.S. § 6-1-1304(2)(k) means the records of an Employee, maintained by the Employer in the context of the Employer-Employee relationship having to do with hiring, promotion, demotion, transfer, lay-off or termination, rates of pay or other terms of compensation, as well as other information maintained because of the Employer-Employee relationship.

"**Human Involved Automated Processing**" means the automated processing of Personal Data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the Processing and (2) has the authority to change or influence the outcome of the Processing.

"**Human Reviewed Automated Processing**" means the automated processing of Personal Data where a human reviews the automated processing, but the level of human engagement does not rise to the level required for Human Involved Automated Processing. Reviewing the output of the automated processing with no meaningful consideration does not rise to the level of Human Involved Automated Processing.

"**Information that a Controller has a reasonable basis to believe the Consumer has lawfully made available to the general public**" as referred to in C.R.S. § 6-1-1303(17)(b) means information that a Consumer has intentionally made available to the general public or information that a Consumer has made available under federal or state law, which may include but is not limited to:

1. Personal Data found in a telephone book, a television or radio program, or a national or local news publication;

2. Personal Data that has been intentionally made available by the Consumer through a website or online service where the Consumer has not restricted the information to a specific audience;

3. A visual observation of an individual's physical presence in a public place by another person, not including data collected by a device in the individual's possession; and

4. A disclosure that has been made to the general public as required by federal, state, or local law.

"**Intimate Image**" means any visual depiction, photograph, film, video, recording, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, that depicts an identified or identifiable person's private parts, or a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy.

"**Noncommercial Purpose**" as referred to in C.R.S. § 6-1-1304(2)(o) includes, but is not limited to, the following activities when conducted by: (a) a state institution of higher education, as defined in C.R.S. § 23-18-102(10), the state, the judicial department of the state, or a county, city and county, or municipality; or (b) a Processor acting on behalf of one or more of the foregoing:

1. Processing activities related to the delivery of services and benefits;

2. Research purposes;

3. Budgeting;

4. Improving operations or the delivery services or benefits;

5. Auditing operations or service or benefit delivery;

6. Sharing Personal Data between these categories of entities for any of these purposes; or

7. Any other purpose related to speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

"**Opt-Out Purpose**" or "**Opt-Out Purposes**" means the categories of Personal Data Processing from which the Consumer may opt out pursuant to C.R.S. § 6-1-1306(1)(a).

"**Personal Data**" is defined as set forth in C.R.S. § 6-1-1303(17), and (a) means information that is linked or reasonably linkable to an identified or identifiable individual; and (b) does not include de-identified data or Publicly Available Information as used in (17)(b).

"**Process**" or "**Processing**" is defined as set forth in C.R.S. § 6-1-1303(18), and means the collection, use, sale, storage, disclosure, analysis, deletion, or modification of Personal Data and includes the actions of a Controller directing a Processor to Process Personal Data.

"**Processor**" is defined as set forth in C.R.S. § 6-1-1303(19), and means a person that Processes Personal Data on behalf of a Controller.

"**Profiling**" is defined as set forth in C.R.S. § 6-1-1303(20), and means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"**Publicly Available Information**" is defined as set forth in C.R.S. § 6-1-1303(17), and does not include:

1. Any Personal Data obtained or processed in in violation of C.R.S. §§ 18-7-107 or 18-7-801;

2. Biometric Data;

3. Genetic Information; or

4. Nonconsensual Intimate Images known to the Controller.

"**Revealing**" as referred to in C.R.S. § 6-1-1303(24)(a) includes Sensitive Data Inferences. For example:

1. While precise geolocation information at a high level may not be considered Sensitive Data, precise geolocation data which is used to infer an individual visited a mosque and is used to infer that individual's religious beliefs is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a). Similarly, precise geolocation data which is used to infer an individual visited a reproductive health clinic and is used to infer an individual's health condition or sex life is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a).

2. While web browsing data at a high level may not be considered Sensitive Data, web browsing data which, alone or in combination with other Personal Data, infers an individual's sexual orientation is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a).

"**Sensitive Data Inference**" or "**Sensitive Data Inferences**" means inferences made by a Controller based on Personal Data, alone or in combination with other data, which are used to indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status.

"**Solely Automated Processing**" means the automated processing of Personal Data with no human review, oversight, involvement, or intervention.

"**Universal Opt-Out Mechanism**" or "**Universal Opt-Out Mechanisms**" means 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), which meets the technical specifications set forth in 4 CCR 904-3, Rule 5.06 pursuant to C.R.S. § 6-1-1313(2).

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. 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, *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 children. For example, they shall use plain, straightforward language and avoid technical or legal jargon.

2. Reasonably accessible to Consumers with Disabilities, including through the use of digital accessibility tools. For notices provided online, the Controller shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference as described at 4 CCR 904-3, Rule 11.02. In other contexts, the Controller shall provide information on how a Consumer with a Disability may access the disclosure or communication or make a request in an alternative format.

3. Available in the languages in which the Controller in its ordinary course provides web pages, interfaces, contracts, disclaimers, sale announcements, and other information to Consumers. Disclosures and communications sent directly to Consumers must be sent in the language in which the Consumer ordinarily interacts with the Controller.

4. Available through a readily accessible interface regularly used in conjunction with the Controller's product or service.

5. Provided in a readable format on all devices through which Consumers normally or regularly interact with the Controller, including on smaller screens and through mobile applications, if applicable.

6. Unless otherwise stated, communicated in a manner by which the Controller regularly interacts with Consumers.

7. Straightforward and accurate, and must not be written or presented in a way that is unfair, deceptive, false, or misleading.

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. 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 4.02 SUBMITTING REQUESTS TO EXERCISE PERSONAL DATA RIGHTS

A. Pursuant to C.R.S. § 6-1-1306(1), a Controller's privacy notice must include specific methods through which a Consumer may submit requests to exercise Data Rights.

B. Any method specified by a Controller pursuant to this rule must comply with each of the following:

1. Consider the ways in which Consumers normally interact with the Controller:

a. A Controller that interacts with Consumers exclusively online and has a direct relationship with a Consumer from whom it collects Personal Data shall only be required to provide an email address for submitting access, correction, deletion, or data portability requests.

b. A Controller that does not fall within subsection 4 CCR 904-3, Rule 4.02(B)(1)(a) shall provide two or more designated methods for submitting a Data Rights request. If a Controller maintains a website, mobile application, or other digital presence, one method for submitting requests shall be through its website, mobile application, or digital interface, such as through a webform;

c. If a Controller interacts with Consumers in person, the Controller shall consider providing an in-person method such as a printed form the Consumer can directly submit or send by mail; a tablet or computer portal that allows the Consumer to complete and submit an online form; or a telephone by which the Consumer can call the Controller's toll-free number.

2. Enable the Consumer to submit the request to the Controller at any time;

3. Comply with requirements for disclosures, notifications, and other communications to Consumers provided in 4 CCR 904-3, Rule 3.02;

4. Use reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, when exchanging information in furtherance of Data Rights requests, considering the volume, scope and nature of Personal Data that may be exchanged; and

5. Be easy for Consumers to execute, requiring a minimal number of steps.

C. The Data Rights request method does not have to be specific to Colorado, so long as the request method:

1. Clearly indicates which rights are available to Colorado Consumers;

2. Provides all Data Rights available to Colorado Consumers;

3. Provides Colorado Consumers a clear understanding of how to exercise their rights; and

4. Meets all other requirements of this part, 4 CCR 904-3, Rule 4.02.

D. When a Consumer submits a Data Rights request, a Controller may only collect Personal Data through the request process if the Personal Data is reasonably necessary to Authenticate the Consumer, respond to the request, or effectuate the Data Rights request.

E. A Controller must not require a Consumer to create a new user account to exercise their Data Rights request, but may require a Consumer to use an existing password-protected account.

Rule 4.03 RIGHT TO OPT OUT

A. A Controller shall comply with an opt-out request by:

1. Ceasing to Process the Consumer's Personal Data for the Opt-Out Purpose(s) as soon as feasibly possible and without undue delay from the date the Controller receives the request, taking into account the size and complexity of the Controller's businesses and burden of operationalizing the opt-out.

    a. If a Controller does not know the identity of a Consumer submitting an online opt-out request, such that the Controller is unable to opt the Consumer out of the Processing of offline or other connected Personal Data, the Controller may request the additional information necessary to do so subject to 4 CCR 904-3, Rules 4.08 and 5.05.

    b. If a Consumer submits a request to exercise more than one Data Right and a Controller is able to complete the opt-out request in a more timely manner than other Data Rights requests, the Controller should complete the opt-out request prior to any other Data Rights request.

2. Maintaining a record of the opt-out request and response, in compliance with 4 CCR 904-3, Rule 6.11.

3. Using agreed upon technical, organizational or other measures or processes to instruct its Processors, pursuant to C.R.S. § 6-1-1305(2)(a), to stop Processing the Personal Data as needed to effectuate the Consumer's opt-out request.

B. To enable a Consumer to exercise the right to opt out of the Opt-Out Purposes provided in C.R.S. § 6-1-1306(1)(a)(I), a Controller must provide the disclosures required by C.R.S. § 6-1-1308(1)(b).

1. A Controller that Sells Personal Data or Processes Personal Data for Targeted Advertising must also provide a clear and conspicuous method for Consumers to exercise the right to opt out of the Processing of Personal Data for each or all of the Opt-Out Purposes, as applicable.

    a. The clear, conspicuous method must be provided either directly or through a link, in a clear, conspicuous, and readily accessible location outside the privacy notice.

2. A Controller Processing Personal Data for Profiling in furtherance of a decision 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, as subject to the opt-out right provided at C.R.S. § 6-1-1306(1)(a)(I), shall provide a clear and conspicuous method for Consumers to exercise the right to opt out of Processing Personal Data for such Profiling at or before the time such Processing occurs.

3. Any clear and conspicuous method for Consumers to exercise the right to opt out of Processing for the Opt-Out Purposes, provided pursuant to this section, must comply with the requirements of 4 CCR 904-3, Rule 4.02(B). If a link is used, it must take a Consumer directly to the opt-out method and the link text must provide a clear understanding of its purpose, for example "Colorado Opt-Out Rights," "Personal Data Use Opt-Out," "Your Opt-Out Rights," "Your Privacy Choices," or "Your Colorado Privacy Choices."

C. An Authorized Agent may exercise a Consumer's opt-out right on behalf of the Consumer, so long as the Controller is able to, with commercially reasonable effort, Authenticate the identity of the Consumer and the Authorized Agent's authority to act on the Consumer's behalf.

D. A Controller may collect the Consumer's Personal Data necessary to effectuate the Consumer's opt-out right, pursuant to 4 CCR 904-3, Rule 4.02(D).

Rule 4.04 RIGHT OF ACCESS

A. A Controller shall comply with an access request by providing the Consumer all the specific pieces of Personal Data it has collected and maintains about the Consumer that are the subject of the request, including without limitation, any Personal Data that the Controller's Processors obtained from the Controller in providing services to the Controller.

1. Specific pieces of Personal Data include final Profiling decisions, inferences, derivative data, marketing profiles, and other Personal Data created by the Controller which is linked or reasonably linkable to an identified or identifiable individual.

B. Personal Data provided in response to an access request must:

1. Be provided in 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.

C. 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.

D. 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.

E. 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.

Rule 4.05 RIGHT TO CORRECTION

A. Consumers have the right to correct inaccuracies in their Personal Data subject to C.R.S. § 6-1-1306(c).

B. A Controller shall comply with a Consumer's correction request by correcting the Consumer's Personal Data in its existing systems, except archive or backup systems. The Controller shall also use agreed upon technical, organizational, or other measures or processes to instruct its Processors, pursuant to C.R.S. § 6-1-1305(2)(a), to make the necessary corrections in their respective systems.

C. If a Controller or Processor stores any Personal Data on archived or backup systems, it may delay compliance with the Consumer's correction request with respect to an archived or backup system until that system is restored to an active system or is next accessed or used.

D. If a Consumer submits a request to exercise their right to correct Personal Data and the requested correction to that Personal Data could be made by the Consumer through the Consumer's account settings, a Controller may respond to the Consumer's request by providing instructions on how the Consumer may correct the Personal Data so long as:

1. The correction process is not unduly burdensome to the Consumer;

2. The instructions meet all requirements of 4 CCR 904-3, Rule 3.02;

3. The Controller's response is compliant with the timing requirements set forth in C.R.S. § 6-1-1306(2)(a); and

4. The process described in the instructions enable the Consumer to make the specific requested correction.

E. A Controller may require the Consumer to provide documentation if necessary to determine whether the Personal Data, or the Consumer's requested correction to the Personal Data, is accurate.

1. When requesting documentation, the Controller must provide the Consumer with a meaningful understanding of why the documentation is necessary.

2. Any documentation provided by the Consumer in connection with the Consumer's right to correction shall only be Processed by the Controller in considering the accuracy of the Consumer's Personal Data.

3. 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 the Consumer's correction request.

4. If the Controller did not receive the Personal Data directly from the Consumer and has no documentation to support the accuracy of the Personal Data, the Consumer's assertion of inaccuracy shall be sufficient to establish that the Personal Data is inaccurate.

5. A Controller, having exhausted the steps above may decide not to act upon a Consumer's correction request if the Controller determines that the contested Personal Data is more likely than not accurate.

a. If a Controller denies a Consumer's correction request based on the Controller's determination that the contested Personal Data is more likely than not accurate, the Controller must describe in documentation required by 4 CCR 904-3, Rule 6.11(A), the Consumer's requested correction to the Personal Data, any documentation requested from and provided by the Consumer in support of the correction request, and the reason for the Controller's determination that the Consumer's documentation was not sufficient to support the Consumer's position.

Rule 4.06 RIGHT TO DELETION

A. A Controller shall comply with a Consumer's deletion request by:

1. Permanently and completely erasing the Personal Data from its existing systems, except archive or backup systems, or de-identifying the Personal Data such that it cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, in accordance with C.R.S. § 6-1-1303(11); and

2. Using agreed upon technical, organizational, or other measures, or processes to instruct its Processors pursuant to C.R.S. § 6-1-1305(2)(b) to delete the Consumer's Personal Data held by the Processors.

B. Notwithstanding 4 CCR 904-3, Rule 4.06(A), a Controller may maintain records of a Consumer's deletion request consistent with 4 CCR 904-3, Rule 6.11 and as needed to effectuate the deletion request.

C. If a Controller or Processor stores any Personal Data on archived or backup systems, it may delay compliance with the Consumer's deletion request with respect to an archived or backup system until that system is restored to an active system or is next accessed or used.

D. A Controller that has obtained Personal Data about a Consumer from a source other than the Consumer shall comply with a Consumer's deletion request with respect to that Personal Data pursuant to C.R.S. § 6-1-1306(d) by (i) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the Consumer's Personal Data remains deleted from the Consumer's records and not using such retained data for any other purpose, or (ii) opting the Consumer out of the Processing of such Personal Data for any purpose except for those exempted pursuant to the provisions of C.R.S. § 6-1-1304.

E. If a Controller complies with a deletion request by opting the Consumer out of Processing under 4.06(D) or does not opt the Consumer out of some Processing of Personal Data because the Processing purpose is exempted pursuant to the provisions of C.R.S. § 6-1-1304, the Controller shall provide the Consumer with the categories of Personal Data that were not deleted along with any applicable exception. The Controller shall not use the Consumer's Personal Data retained for any other purpose than provided for by the applicable exception.

Rule 4.07 RIGHT TO DATA PORTABILITY

A. To comply with a data portability request, a Controller must transfer to a Consumer the Personal Data it has collected and maintains about the Consumer through a secure method in a commonly used electronic format that, to the extent technically feasible, is readily usable and allows the Consumer to transmit the Personal Data to another entity without hindrance.

B. Pursuant to C.R.S. § 6-1-1306(1)(e), a Controller is not required to provide Personal Data to a Consumer in a manner that would disclose the Controller's trade secrets. When complying with a

request to access Personal Data in a portable format, Controllers must provide as much data as possible in a portable format without disclosing the trade secret.

1. For example, if sharing both raw or unedited Personal Data along with related inferences or derived Personal Data in an Excel file would reveal a trade secret, the Controller may provide either set of Personal Data in an Excel file, so long as it is clear to the Consumer that the Controller maintains both types of Personal Data.

Rule 4.08 AUTHENTICATION

A. Pursuant to C.R.S. § 6-1-1306(1), a Controller shall use a commercially reasonable method for authenticating the identity of every Consumer submitting any Data Right request, and the authority of every Authorized Agent submitting an opt-out request on behalf of a Consumer pursuant to C.R.S. § 6-1-1306(1)(a)(II).

1. To determine if an authentication method is commercially reasonable, the Controller shall consider the Data Rights exercised, the type, sensitivity, value, and volume of Personal Data involved, the level of possible harm that improper access or use could cause to the Consumer submitting the Data Right request and the cost of authentication to the Controller. A Controller must avoid methods that place an unreasonable burden on the Consumer submitting a Data Right request, or Authorized Agent submitting an opt-out request on behalf of a Consumer.

B. When possible, a Controller shall avoid requesting additional Personal Data to Authenticate a Consumer unless the Controller cannot Authenticate the Consumer using the Personal Data already maintained by the Controller.

C. Personal Data obtained to Authenticate a Consumer may only be used to Authenticate the Consumer submitting the Data Right request, pursuant to C.R.S. § 6-1-1306(1), or to Authenticate an Authorized Agent's authority, pursuant C.R.S. § 6-1-1306(1)(a)(II), and must be deleted as soon as practical after Processing the Consumer's request, except as required by 4 CCR 904-3, Rule 6.11, or as otherwise required.

D. A Controller shall implement reasonable security measures, consistent with 4 CCR 904-3, Rule 6.09, to protect Personal Data exchanged to Authenticate a Consumer or to Authenticate an Authorized Agent's authority, considering the type, value, sensitivity, and volume of information exchanged and the level of possible harm improper access or use could cause to the Consumer submitting a Data Right request.

E. A Controller shall not require the Consumer or Authorized Agent to pay a fee for authentication. For example, a Controller may not require a Consumer to provide a notarized affidavit for authentication unless the Controller compensates the Consumer for the cost of notarization.

F. If a Controller cannot Authenticate the Consumer submitting a Data Right request using commercially reasonable efforts, the Controller is not required to comply with the Consumer's request. The Controller shall inform the Consumer that their identity could not be authenticated, provide information on how to remedy any deficiencies, and may request additional Personal Data if reasonably necessary to Authenticate the Consumer.

Rule 4.09 RESPONDING TO CONSUMER REQUESTS

A. A Controller must respond to a Consumer's Data Right request in compliance with the timing provisions of C.R.S. § 6-1-1306(2)(a)-(b).

B. A Controller does not have to comply with an authenticated Consumer request to access, correct, delete, or provide Personal Data in a portable format, to the extent that the Personal Data at issue meets the requirements of the exceptions in C.R.S. § 6-1-1307(1)(b) and 1307(3).

C. If a Controller decides not to act on a Consumer's Data Right request, the Controller's response to the Consumer must include the grounds for denial, including but not limited to (1) any conflict with federal or state law; (2) if the Controller relied on an exception to the Colorado Privacy Act found at C.R.S. § 6-1-1304(2), a description of the exception; (3) the Controller's inability to Authenticate the Consumer's identity; (4) any factual basis for a Controller's good-faith claim that compliance is impossible; or (5) any basis for a good-faith, documented belief that the request is fraudulent or abusive.

1. If a Controller denies a Consumer Data Right request based on inability to Authenticate, the Controller must describe in documentation required by 4 CCR 904-3, Rule 6.11 their reasonable efforts to authenticate and why they were unable to do so.

2. A Controller that decides not to act on a Consumer's request must also provide instructions on how to appeal the Controller's decision in accordance with C.R.S. § 6-1-1306(3).

D. When a Controller complies with a Consumer's Personal Data Right request, the Controller shall also use agreed upon technical, organizational, or other measures or processes, to instruct its Processors, pursuant to C.R.S. § 6-1-1305(2)(a), to fulfill requests relating to Personal Data held by the Processors.

E. Controllers must maintain all documentation as required by 4 CCR 904-3, Rule 6.11 of these rules.

F. If a Consumer or Authorized Agent submits a request to opt out of the Processing of a Consumer's Personal Data for an Opt-Out Purpose in a manner that is not one of the Controller's opt-out request methods, or submits a Data Right request that is otherwise deficient in a manner unrelated to the Authentication process, the Controller shall either: (1) treat the request as if it had been submitted in accordance with the Controller's specified request methods, or (2) provide the Consumer or Authorized Agent that submitted the request with information on how to submit the request or remedy any deficiencies in the request.

PART 5 UNIVERSAL OPT-OUT MECHANISM

Rule 5.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in Part 5 is C.R.S. §§ 6-1-108(1), 6-1-1306, and 6-1-1313. The purpose of this Part 5 is to provide technical and other specifications for Universal Opt-Out Mechanisms.

Rule 5.02 RIGHTS EXERCISED

A. Consumers may exercise their right to opt out of the Processing of Personal Data concerning the Consumer for purposes of Targeted Advertising or the Sale of Personal Data through a user-selected Universal Opt-Out Mechanism that meets the technical and other specifications provided in this Rule 5.

B. The purpose of a Universal Opt-Out Mechanism is to provide Consumers with a simple and easy-to-use method by which Consumers can automatically exercise their opt-out rights with all Controllers they interact with without having to make individualized requests with each Controller.

C. A Universal Opt-Out Mechanism may:

1. Express a Consumer's choice to opt out of the Processing of Personal Data for both the Processing of Personal Data for purposes of Targeted Advertising and Sale of Personal Data; or

2. Express a Consumer's choice to opt out of the Processing of Personal Data for only one specific purpose, either Targeted Advertising or Sale of Personal Data alone.

Rule 5.03 NOTICE AND CHOICE FOR UNIVERSAL OPT-OUT MECHANISMS

A. If a platform, developer, or provider provides a Universal Opt-Out Mechanism, that platform, developer, or provider shall make clear to the Consumer, whether in its configuration or disclosures to the public, that the mechanism is meant to allow the Consumer to exercise the right to opt out of the Processing of Personal Data for one specific purpose, either Targeted Advertising or Sale of Personal Data, or both purposes. These notices provided to the Consumer:

1. Shall comply with the requirements for disclosures and communications to Consumers provided in 4 CCR 904-3, Rule 3.02;

2. If applicable, shall state that the Universal Opt-Out Mechanism has been recognized by the Colorado Attorney General;

3. Shall clearly describe any limitations that may be applicable to the mechanism, for example:

a. That the mechanism will allow a consumer to exercise the opt-out right for only one specific purpose, either Targeted Advertising or Sale of Personal Data; or

b. That the mechanism applies only to a single browser or device.

4. Need not be tailored only to Colorado or refer to Colorado or to any other specific provisions of these rules or the Colorado Privacy Act, provided the mechanism meets the requirements of 4 CCR 904-3, Rule 5.03(A)(1)-(3).

a. Example: A platform, developer, or provider discloses that its Universal Opt-Out Mechanism permits consumers to exercise "any and all opt-out rights available to you under state laws," and complies with the other requirements of this Rule 5.03(A) but makes no mention of Colorado nor recites any section of these rules or the Colorado Privacy Act. These disclosures satisfy the requirements of this Rule 5.03(A).

B. A valid Universal Opt-Out Mechanism must represent the Consumer's affirmative, freely given, and unambiguous choice to opt out of the Processing of Personal Data for the purposes listed at C.R.S. § 6-1-1306(1)(a)(IV)(A) and (B). Controllers are not obligated to honor Consumer rights requests for purposes other than those listed at C.R.S. § 6-1-1306(1)(a)(IV)(A) and (B) when transmitted through a Universal Opt-Out Mechanism.

C. The platform, developer, or provider that provides a Universal Opt-Out Mechanism is not obligated to authenticate that a user is a Resident of Colorado. The platform, developer, or provider may provide such authentication capabilities if it chooses.

Rule 5.04 DEFAULT SETTINGS FOR UNIVERSAL OPT-OUT MECHANISMS

A. To comply with C.R.S. § 6-1-1313(2), a Universal Opt-Out Mechanism may not be the default setting for a tool that comes pre-installed with a device, such as a browser or operating system.

1. Example: An operating system manufacturer bundles a browser pre-installed with every device shipped with the operating system. The browser sends a Universal Opt-Out mechanism signal by default and never asks the Consumer to enable this setting. The Consumer's decision to use this browser does not represent the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism because it is a default choice. This is so even if the marketing for the operating system touts its privacy protective features.

2. Example: An operating system manufacturer bundles a browser and apps pre-installed with every device shipped with the operating system. The first time a Consumer runs a browser or app, the operating system asks the Consumer specifically and clearly whether they want to opt out of the Sale of their Personal Data using a Universal Opt-Out Mechanism signal when using the browser or app. No choice is pre-selected, meaning the Consumer is forced to decide. The Consumer's decision to select "yes" to enable the signal to opt out of the Sale of Personal Data represents the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism.

B. Notwithstanding 4 CCR 904-3, Rule 5.04(A), a Consumer's decision to adopt a tool that does not come pre-installed with a device, such as a browser or operation system, but is marketed as a tool that will exercise a user's rights to opt out of the Processing of Personal Data using a Universal Opt-Out Mechanism, shall be considered the Consumer's affirmative, freely given, and unambiguous choice to use a Universal Opt-Out Mechanism. The marketing for such a tool may also describe functionality other than the exercise of opt out rights and it need not refer specifically to opt-out rights in the State of Colorado.

1. Example: A browser manufacturer markets its browser as a "privacy friendly" browser, prominently highlighting that the browser sends a Universal Opt-Out Mechanism signal by default. The browser does not come pre-installed with a device or operating system and must be installed by the Consumer. The Consumer's decision to use this browser represents the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism. The Consumer need not be given an explicit choice about whether to use the Universal Opt-Out Mechanism in this example.

Rule 5.05 PERSONAL DATA USE LIMITATIONS

A. A platform, developer, or provider providing a Universal Opt-Out Mechanism shall not use, disclose, or retain any Personal Data collected from the Consumer in connection with the Consumer's utilization of the mechanism for any purpose other than sending or processing the opt-out preference. For example, the fact that a particular device sends a Universal Opt-Out Mechanism may not be used as part of a digital fingerprint to later identify that device.

B. When processing a Universal Opt-Out Mechanism, a Controller may not require the collection of additional Personal Data beyond that which is strictly necessary to authenticate a Consumer is a resident of Colorado determine that the mechanism represents a legitimate request to opt out of the Processing of Personal Data as permitted by C.R.S. § 6-1-1306(1)(a)(IV), or comply with the authentication mandates of the law of another jurisdiction specifically regarding universal opt-out mechanisms or signals.

1. Example: The law of a state other than Colorado obligates Controllers to gather specific pieces of information from a user before the Controller honors the use of a Universal Opt-Out Mechanism by that user. This additional information may be gathered while processing a Universal Opt-Out Mechanism, even if is not otherwise "strictly necessary to

authenticate a Consumer is a resident of Colorado or determine that the mechanism represents a legitimate request".

C. Notwithstanding 4 CCR 904-3, Rule 5.05(B), a Controller may provide the Consumer with an option to provide additional Personal Data only if it will extend the recognition of the Consumer's use of the Universal Opt-Out Mechanism across platforms, devices, or offline. For example, a Controller may give the Consumer the option to provide their phone number or email address so that the Universal Opt-Out Mechanism or signal can apply to offline Sale of Personal Data or link the Consumer's opt-out choice across devices. Any information provided by the Consumer for this purpose shall not be used, disclosed, or retained for any purpose other than processing the opt-out request.

D. The Controller shall implement and maintain reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, in Processing any Personal Data relating to the Consumer's use of a Universal Opt-Out Mechanism.

Rule 5.06 TECHNICAL SPECIFICATION

A. A Universal Opt-Out Mechanism must allow for Consumers to automatically communicate their opt-out choice with multiple Controllers.

1. The Universal Opt-Out Mechanism may communicate a Consumer's opt-out choice by sending an opt-out signal. The signal must be in a format commonly used and recognized by Controllers. An example would be an HTTP header field or JavaScript object.

B. The Universal Opt-Out Mechanism must allow Consumers to clearly communicate one or more opt-out rights available under C.R.S. § 6-1-1306(1)(a)(IV).

1. The Universal Opt-Out Mechanism may allow for a Consumer to opt out of Processing for one or more of the Opt-Out Purposes.

C. The Universal Opt-Out Mechanism must store, Process, and transmit any Consumer Personal Data using reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09.

D. A Universal Opt-Out Mechanism must not prevent the Controller's ability to determine:

1. Whether a Consumer is a Resident of the State of Colorado; or

2. That the Universal Opt-Out Mechanism represents a legitimate request to opt out of the Processing of Personal Data.

E. A Universal Opt-Out Mechanism must not unfairly disadvantage any Controller. For example, a Universal Opt-Out Mechanism may not engage in self-dealing benefiting the creator of the Universal Opt-Out Mechanism over other Controllers.

Rule 5.07 SYSTEM FOR RECOGNIZING UNIVERSAL OPT-OUT MECHANISMS

A. The Colorado Department of Law shall maintain a public list of Universal Opt-Out Mechanisms that have been recognized to meet the standards of this subsection. The initial list shall be released no later than January 1, 2024 and shall be updated periodically.

B. The goal of the public list is to simplify the options facing Controllers, Consumers, and other actors.

C. To be recognized, a Universal Opt-Out Mechanism must at a minimum meet these standards:

1. Comply with all of the technical and other specifications of Rule 5; and

2. Not create Consumer or Controller confusion about the similarities and differences between Universal Opt-Out Mechanisms on the public list.

D. The Colorado Department of Law may consider additional factors when determining which Universal Opt-Out Mechanisms to recognize. These include but are not limited to:

1. Commercial adoption by Consumers or Controllers;

2. Ease and cost of use, implementation, and detection by Consumers and Controllers;

3. Whether the Universal Opt-Out Mechanism has been approved by a widely recognized, legitimate standards body after broad multistakeholder participation in the standards-making process; and

4. Whether the Universal Opt-Out Mechanism is based on an open system or standard, and whether such standard is free for adoption by device, operating system, browser, and other manufacturers, Controllers, or Consumers without permission or on fair, reasonable, and non-discriminatory terms.

E. The public list shall describe recognized Universal Opt-Out Mechanisms in enough technical detail to permit Controllers to identify them when used by Consumers.

F. The Colorado Department of Law will allow Controllers six (6) months to recognize a Universal Opt-Out Mechanism once that Mechanism is added to the public list.

Rule 5.08 OBLIGATIONS ON CONTROLLERS

A. Effective July 1, 2024,

1. A Controller that receives an opt-out request through a Universal Opt-Out Mechanism shall treat such as a valid request to opt out of the Processing of Personal Data for purposes of Targeted Advertising, Sale of Personal Data, or both purposes, as indicated by the mechanism, for the associated browser or device, and, if known, for the Consumer.

2. After receiving a valid opt-out request through the use of a Universal Opt-Out Mechanism, a Controller shall continue to treat the browser, device, and Consumer as having exercised opt-out rights until the Consumer Consents to the Sale of Personal Data or Processing of Personal Data for Targeted Advertising, as specified in 4 CCR 904-3, Rule 5.09.

3. A Controller shall be capable of recognizing any Universal Opt-Out Mechanism reflected in the public list maintained by the Colorado Department of Law pursuant to subsection 4 CCR 904-3, Rule 5.07 provided the Controller has had at least six months' notice of the addition of new mechanisms. For example, in the case of a recognized Universal Opt-Out Mechanism sent as a signal, the Controller must listen for the signal.

B. A Controller may also recognize Universal Opt-Out Mechanisms that are not reflected in the public list maintained by the Colorado Department of Law pursuant to subsection 4 CCR 904-3, Rule 5.07.

C. Notwithstanding 4 CCR 904-3, Rule 5.08(A), a Controller may choose to honor an opt-out request received through a Universal Opt-Out Mechanism prior to July 1, 2024, pursuant to C.R.S. § 6-1-1306(a)(IV)(A).

D. Unless a Controller is Authenticating a Consumer as permitted by C.R.S. § 6-1-1313(2)(f), a Controller may not require a Consumer to login or otherwise Authenticate themself as a condition of recognizing the Consumer's use of a Universal Opt-Out Mechanism. A Controller may not subject a Consumer to undertake any authentication actions that are unnecessary or unnecessarily burdensome.

E. A Controller may display in a conspicuous manner if it has Processed the Consumer's opt-out preference signal. For example, the Controller may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or Consumer utilizing a Universal Opt-Out Mechanism visits the website.

F. Pursuant to C.R.S. § 6-1-1313(2)(f), a Controller may authenticate that the user sending an opt-out request through a Universal Opt-Out Mechanism is a Resident of Colorado, but they are not obligated to do so.

Rule 5.09 CONSENT AFTER UNIVERSAL OPT-OUT

A. A Controller may enable a Consumer to Consent to Processing that the Consumer has opted-out of using a Universal Opt-Out mechanism, so long as the Controller's request for Consent complies with the Consent requirements provided in C.R.S. § 6-1-1306(1)(a)(IV)(C), and 4 CCR 904-3, Rule 7.05.

B. A Controller shall not interpret the absence of a Universal Opt-Out Mechanism signal after the Consumer previously utilized a Universal Opt-Out Mechanism as Consent to opt back in.

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. 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 6.02 PRIVACY NOTICE PRINCIPLES

A. A privacy notice shall provide Consumers with a meaningful understanding and accurate expectations of how their Personal Data will be Processed. It shall also inform Consumers about their rights under the Colorado Privacy Act and provide any information necessary for Consumers to exercise those rights.

B. A Controller is not required to provide a separate Colorado-specific privacy notice or section of a privacy notice as long as the Controller's privacy notice meets all requirements of this section and makes clear that Colorado Consumers are entitled to the rights provided by C.R.S. § 6-1-1306.

C. A privacy notice shall comply with all requirements for disclosures and communications to Consumers provided in 4 CCR 904-3, Rule 3.02.

D. A privacy notice must be clear. Information contained in a privacy notice shall be:

1. Concrete and definitive, avoiding abstract or ambivalent terms that may lead to varying interpretations.

2. Clearly labeled, such that Consumers seeking to understand a Controller's Processing activities or how to exercise their Data Rights can easily access the section of the privacy notice containing relevant information.

E. A privacy notice must be easily accessible. A privacy notice must be:

1. Posted online through a conspicuous link using the word "privacy" on the Controller's website homepage or on a mobile application's app store page or download page. A Controller that maintains an application on a mobile or other device shall also include a link to the privacy notice in the application's settings menu.

a. A Controller that does not operate a website shall make the privacy 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.

F. A privacy notice must be specific. The level of specificity in a privacy notice should enable a Consumer to understand, in advance or at the time of the Processing, the scope of the Controller's Processing operations, such that a Consumer should not be taken by surprise at a later point about Personal Data that has been collected and the ways in which Personal Data has been Processed.

Rule 6.03 PRIVACY NOTICE CONTENT

A. A privacy notice must include the following information:

1. A comprehensive description of the Controller's online and offline Personal Data Processing practices, including but not limited to the following, linked in a way that gives Consumers a meaningful understanding of how each category of their Personal Data will be used when they provide that Personal Data to the Controller for a specified purpose:

a. The categories of Personal Data Processed, including, but not limited to, whether Personal Data of a Child or other Sensitive Data is Processed.

i. Categories shall be described in a level of detail that provides Consumers a meaningful understanding of the type of Personal Data Processed. For example, categories of Personal Data described at a sufficiently granular level of detail include, but are not limited to: "contact information," "government issued identification numbers," "payment information", "Information from Cookies," "data revealing religious affiliation," and "medical data."

b. The Processing purpose described in a level of detail that gives Consumers a meaningful understanding of how each category of their Personal Data is used when provided for that Processing purpose.

c. Whether the Personal Data provided for a specific purpose will be sold or used for Targeted Advertising or Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer.

d. Categories of Personal Data that the Controller Sells to or shares with Third Parties, if any.

e. Categories of Third Parties to whom the Controller sells, or with whom the Controller shares Personal Data, if any. Categories of Third Parties must be described in a level of detail that gives Consumers a meaningful understanding of the type of, business model of, or processing conducted by the Third Party.

i. For example, categories of Third Parties described in a sufficiently granular level of detail include, but are not limited to: "analytics companies," "data brokers," "third-party advertisers," "payment processors," "lenders," "other merchants," and "government agencies."

2. If a Controller's Processing activity involves the Processing of Personal Data for the purpose of Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer, all disclosures required by 4 CCR 904-3, Rule 9.03.

3. A list of the Data Rights available.

4. A description of the methods through which a Consumer may submit requests to exercise Data Rights, as required by C.R.S. § 6-1-1306(1) and 4 CCR 904-3, Rule 4.02, including:

a. Instructions on how to use each method.

b. Instructions on how an Authorized Agent may submit a request to opt out of the Processing of Consumer Personal Data on a Consumer's behalf pursuant to C.R.S. § 6-1-1306(1)(a)(II).

c. A clear and conspicuous method to exercise the right to opt out of the Processing of Personal Data concerning the Consumer pursuant to C.R.S. § 6-1-1306(1)(a)(I) and (1)(a)(III), or links to any online method, such as a webform or portal, consistent with 4 CCR 904-3, Rule 4.03.

d. A description of the commercially reasonable process the Controller uses to Authenticate the identity of a Consumer exercising a Data Right request or to Authenticate the authority of an Authorized Agent exercising the right to opt out on a Consumer's behalf.

e. Effective July 1, 2024, an explanation of how requests to opt out using Universal Opt-Out Mechanisms will be processed.

5. If a Controller will delete Sensitive Data Inferences within twenty-four (24) hours pursuant to 4 CCR 904-3, Rule 6.10, a description of the Sensitive Data Inferences subject to this provision and the retention and deletion timeline for such Sensitive Data Inferences.

6. A Controller's contact information.

7. Instructions on how a Consumer may appeal a Controller's action in response to the Consumer's request, as contemplated by C.R.S. § 6-1-1306(3).

8. The date the privacy notice was last updated.

Rule 6.04 CHANGES TO A PRIVACY NOTICE

A. A Controller shall notify Consumers of material changes to a privacy notice. Such changes to a privacy notice shall be communicated to Consumers in a manner by which the Controller regularly interacts with Consumers.

1. Material changes may include, but are not limited to, changes to: (1) categories of Personal Data Processed; (2) Processing purposes; (3) a Controller's identity; (4) the act of sharing of Personal Data with Third Parties; (5) categories of Third Parties Personal Data is shared with; or (6) methods by which Consumers can exercise their Data Rights request.

B. If a material change rises to the level of a secondary use, a Controller must obtain Consent from a Consumer pursuant to 4 CCR 904-3, Rules 7.02-7.05 in order to Process Personal Data that was collected before the change to the privacy notice for that Secondary Use.

Rule 6.05 LOYALTY PROGRAMS

A. Pursuant to 6-1-1308(1)(d), a Controller is not prohibited from offering Bona Fide Loyalty Program Benefits to a Consumer based on the Consumer's voluntary participation in a Bona Fide Loyalty Program.

B. If a Consumer exercises their right to delete Personal Data such that it is impossible for the Controller to provide a certain Bona Fide Loyalty Program Benefit to the Consumer, the Controller is no longer obligated to provide that Bona Fide Loyalty Benefit to the Consumer. However, the Controller shall provide any available Bona Fide Loyalty Program Benefit for which the deleted Personal Data is not necessary.

C. If a Consumer exercises their right to opt out of the Sale of Personal Data or Processing of Personal Data for Targeted Advertising, such that the exchange of Personal Data needed to obtain a Bona Fide Loyalty Program Benefit through a Bona Fide Loyalty Program Partner is no longer possible, the Controller is no longer obligated to provide that Bona Fide Loyalty Program Benefit to the Consumer.

1. If the Controller's Bona Fide Loyalty Program offers Bona Fide Loyalty Program Benefits that are unrelated to the exchange of Personal Data with a Bona Fide Loyalty Program Partner, the Controller shall continue to provide those Benefits to a Consumer who opts out of the Sale of Personal data or Processing of Personal Data for Targeted Advertising.

2. The sale of Personal Data or Processing of Personal Data for Targeted Advertising that is unrelated to sharing of information with a Bona Fide Loyalty Program Partner is a Secondary Use that requires Consent pursuant to 4 CCR 904-3, Rule 6.08.

D. If a Consumer refuses to Consent to the Processing of Sensitive Data necessary for a personalized Bona Fide Loyalty Program Benefit, the Controller is no longer obligated to provide that personalized Bona Fide Loyalty Program Benefit. However, the Controller shall provide any available, non-personalized Bona Fide Loyalty Program Benefit for which the Sensitive Data is not necessary. A Controller may not condition a Consumer's participation in a Bona Fide Loyalty Program on the Consumer's Consent to Process Sensitive Data unless the Sensitive Data is required for all Bona Fide Loyalty Program Benefits.

E. If a Consumer's decision to exercise a Data Right impacts the Consumer's membership in a Bona Fide Loyalty Program, the Controller shall notify the Consumer of the impact of the Consumer's decision in conformance with 4 CCR 904-3, Rule 3.02 and at least twenty-four (24) hours before discontinuing the Consumer's Bona Fide Loyalty Program Benefit or membership, and must provide a reference or link to the information required by subparagraph F, below.

F. Loyalty Program Disclosures

1. In addition to all other disclosures required by 4 CCR 904-3, Rules 6.03 and 7.03, a Controller maintaining a Bona Fide Loyalty Program must provide the following

disclosures at the point of program registration, either directly, or in the form of a link to the specific section of a privacy notice or terms and conditions containing such information:

a. The categories of Personal Data or Sensitive Data collected through the Bona Fide Loyalty Program that will be Sold or Processed for Targeted Advertising, if any;

b. Categories of Third Parties that will receive the Consumer's Personal Data and Sensitive Data, provided in the level the detail described in 4 CCR 904-3, Rule 6.03(a)(1)(e), including whether Personal Data will be provided to Data Brokers;

c. A list of any Bona Fide Loyalty Program Partners, and the Bona Fide Loyalty Program Benefits provided by each Bona Fide Loyalty Program Partner.

d. If a Controller claims that a Consumer's decision to delete Personal Data makes it impossible to provide a Bona Fide Loyalty Program Benefit, then the Controller shall provide an explanation of why the deletion of Personal Data makes it impossible to provide a Bona Fide Loyalty Program Benefit.

e. If a Controller claims that a Consumer's Sensitive Data is required for a Bona Fide Loyalty Program Benefit, then the Controller shall provide an explanation of why the Sensitive Data is required for a Bona Fide Loyalty Program Benefit.

2. Bona Fide Loyalty Program terms and requests for Consent to Process Sensitive Data or Personal Data in connection with the Bona Fide Loyalty Program shall also include a link to the Controller's privacy notice.

G. Example: A Consumer joins a grocery store's Bona Fide Loyalty Program that includes both personalized and non-personalized Bona Fide Loyalty Program Benefits. The grocery store asks the Consumer for Consent to collect Sensitive Data about the Consumer in order to provide personalized Bona Fide Loyalty Program Benefits. When the Consumer refuses Consent, the Controller gives timely notice to the Consumer that it will not provide the personalized Bona Fide Loyalty Program Benefits, but will continue to provide non-personalized Bona Fide Loyalty Program Benefits. Moving forward, the Controller provides only the non-personalized Bona Fide Loyalty Program Benefits following the Consumer's decision to continue to refuse Consent to the collection of Sensitive Data. The Controller is not acting impermissibly because the grocery store is still providing all available non-personalized Bona Fide Loyalty Program Benefits and did not condition the Consumer's participation in the Bona Fide Loyalty Program on the Consumers Consent to process Sensitive Data that is not required for personalized Bona Fide Loyalty Program Benefits.

H. Example: A Consumer joins a hotel chain's Bona Fide Loyalty Program, which provides points that can be applied to obtain discounts for that hotel chain, and for a popular restaurant chain that is not otherwise affiliated with the hotel chain. The restaurant chain requires the hotel chain to provide the Personal Data of each Consumer who wishes to apply the hotel chain's points to obtain restaurant discounts. When the Consumer opts out of the Sale of Personal Data and Processing of Personal Data for Targeted Advertising, the Controller is unable to provide the required information to the restaurant chain. The Controller may discontinue the Bona Fide Loyalty Program Benefit that allows Consumers to use points for discounts for the restaurant chain. However, the hotel chain must still provide all available Bona Fide Loyalty Benefits to be used at the hotel chain.

I. Example: A Consumer joins a retailer's Bona Fide Loyalty Program that offers discounts on products based on the Consumer's purchase history. The retailer wishes to fund the loyalty

program, in part, by selling the Consumer's purchase history to a Data Broker. The retailer must obtain the Consumer's consent to Sell the Consumer's Personal Data to the Data Broker because selling Personal Data obtained through a Bona Fide Loyalty Program to a Data Broker is a secondary use.

J. Example: A Consumer exercises their right to opt out of the Processing of Personal Data for Targeted Advertising. An online gaming company gives the Consumer fewer free games through the company's service, arguing that the additional free games are for members of its loyalty program, which requires the use of Personal Data for Targeted Advertising. The company's differential treatment is prohibited if the Processing of Personal Data is not necessary to provide the additional games. However, if the free games are provided by a Bona Fide Loyalty Program Partner that requires the Consumer data for Targeted Advertising through a co-marketing agreement with the Controller, the differential treatment may be appropriate.

Rule 6.06 PURPOSE SPECIFICATION

A. Controllers shall specify the express purposes for which each category of Personal Data is collected and Processed in both external disclosures to Consumers, including privacy notices required by C.R.S. § 6-1-1308(1), as well as in any internal documentation required by this Part 6.

B. The express purpose must be described in a level of detail that gives Consumers a meaningful understanding of how each category of their Personal Data is used when provided for that Processing purpose.

C. If Personal Data is collected and Processed for more than one purpose, Controllers should specify each unrelated purpose with enough detail to allow Consumers to understand each individual, unrelated purpose.

1. Controllers should not identify one broad purpose to justify numerous Processing activities that are only remotely related.

2. Controllers should not specify one broad purpose to cover potential future Processing activities that are only remotely related.

3. Controllers should not specify so many purposes for which Personal Data could potentially be processed to cover potential future processing activities that the purpose becomes unclear or uninformative.

D. If the Processing purpose has evolved beyond the original express purpose such that it becomes a distinct purpose that is no longer reasonably necessary to or compatible with the original express purpose, the Controller must review and update all related disclosures and documentation as necessary.

Rule 6.07 DATA MINIMIZATION

A. To ensure all Personal Data collected is reasonably necessary for the specified purpose, Controllers shall carefully consider each Processing purpose and determine the minimum Personal Data that is necessary, adequate, or relevant for the express purpose or purposes.

B. Personal Data should only be kept in a form which allows identification of Consumers for as long as is necessary for the express Processing purpose(s). To ensure that the Personal Data are not kept longer than necessary, adequate, or relevant, Controllers shall set specific time limits for erasure or to conduct a periodic review.

1. Any Personal Data determined to no longer be necessary, adequate, or relevant to the express Processing purpose(s) shall be deleted by the Controller and any Processors that the Controller has shared the Personal Data with.

2. Biometric Identifiers, a digital or physical photograph of a person, an audio or voice recording containing the voice of a person, or any Personal Data generated from a digital or physical photograph or an audio or video recording held by a Controller shall be reviewed at least once a year to determine if its storage is still necessary, adequate, or relevant to the express Processing purpose. Such assessment shall be documented according to 4 CCR 904-3, Rule 6.11.

3. Sensitive Data for which Controllers no longer have consent to Process, should be deleted or otherwise rendered permanently anonymized or inaccessible within a reasonable period of time after withdrawal of Consent.

C. A Controller shall not collect Personal Data other than those disclosed in its required privacy notice. If the Controller intends to collect additional Personal Data the Controller shall revise its privacy notice, and notify Consumers of the change to its privacy notice pursuant to 4 CCR 904-3, Rule 6.04.

Rule 6.08 SECONDARY USE

A. The specified Processing purpose is the purpose disclosed to Consumers at or before the time the Personal Data is collected or processed from Consumers. Such disclosure shall be included in any required privacy notice or Consent disclosure.

B. Before Processing Personal Data for purposes that are not reasonably necessary to or compatible with specified Processing purpose(s) disclosed on or after July 1, 2023, the Controller must obtain Consent consistent with C.R.S. § 6-1-1308 and 4 CCR 904-3, Rules 7.02-7.05.

C. When considering if the new Processing purpose is reasonably necessary to or compatible with the original specified purpose(s), Controllers may consider the following, as applicable:

1. The reasonable expectation of an average Consumer concerning how their Personal Data would be Processed once it was collected;

2. The link between the original specified purpose(s) for which the data was collected and the purpose(s) of further Processing;

3. The relationship between the Consumer and the Controller and the context in which the Personal Data was collected;

4. The type, nature, and amount of the Personal Data subject to the new Processing purpose;

5. The type and degree of possible consequence or impact to the Consumer of the new Processing purpose;

6. The identity of the entity conducting the new Processing purposes, e.g., the same or different Controller, or a Third Party; and

7. The existence of additional safeguards for the Personal Data, such as encryption or pseudonymization.

Rule 6.09 DUTY OF CARE

A. Personal Data must be Processed in a manner that ensures reasonable and appropriate administrative, technical, organizational, and physical safeguards of Personal Data collected, stored, and Processed.

B. When determining reasonable and appropriate safeguards, Controllers should consider:

1. Applicable industry standards and frameworks;

2. The nature, size, and complexity of the Controller's organization;

3. The sensitivity and amount of Personal Data;

4. The original source of Personal Data;

5. The risk of harm to Consumers resulting from unauthorized or unlawful access, use, or degradation of the Personal Data; and

6. The burden or cost of safeguards to protect Personal Data from harm assessed in 4 CCR 904-3, Rule 6.09(B)(5).

C. Reasonable and appropriate administrative, technical, organizational, and physical safeguards must be designed to:

1. Protect against unauthorized or unlawful access to or use of Personal Data and the equipment used for the Processing and against accidental loss, destruction, or damage;

2. Ensure the confidentiality, integrity, and availability of Personal Data collected, stored, and Processed;

3. Identify and protect against reasonably anticipated threats to security or the integrity of information; and

4. Oversee compliance with data security policies by the Controller and Processors through reasonable requirements.

D. Reasonable and appropriate administrative, technical, organizational, and physical safeguards to secure Personal Data include but are not limited to those measures provided by C.R.S. § 6-1-713.5 and C.R.S. § 24-73-102, as interpreted by state courts and administrative orders.

Rule 6.10 DUTY REGARDING SENSITIVE DATA

A. Controllers must obtain Consent to Process Sensitive Data, including Sensitive Data Inferences, consistent with C.R.S. § 6-1-1308(7) and 4 CCR 904-3, Rules 7.02-7.05.

B. Controllers may be exempt from obtaining Consent to Process Sensitive Data Inferences from Consumers over the age of thirteen (13) only if:

1. The Processing purpose of such Personal Data would be obvious to a reasonable Consumer based on the context of the collection and use of the Personal Data, and the relationship between the Controller and Consumer;

2. Sensitive Data Inferences are permanently deleted within twenty-four (24) hours of collection or of the completion of the Processing activity, whichever comes first;

3. Sensitive Data Inferences are not transferred, sold, or shared with any Processors, Affiliates, or Third-Parties; and

4. The Personal Data and any Sensitive Data Inferences are not Processed for any purpose other than the express purpose disclosed to the Consumer.

C. If a Controller will delete Sensitive Data Inferences within twenty-four (24) hours, pursuant to this section, they must (1) include description of the Sensitive Data Inferences subject to this provision and the retention and deletion timeline for such Sensitive Data Inferences in its privacy notice, pursuant to 4 CCR 904-3, Rule 6.03, and (2) include the details of the deletion and verification process in the Controller's Data Protection Assessment, pursuant to 4 CCR 904-3, Rule 8.04.

Rule 6.11 DOCUMENTATION CONCERNING DUTIES OF CONTROLLERS

A. Controllers shall maintain records of all Consumer Data Rights requests made pursuant to C.R.S. § 6-1-1306 for at least twenty-four (24) months. Such records shall include, at a minimum, each of the following:

1. The date of request;

2. The Consumer Data Rights request type;

3. The date of the Controller's response;

4. The nature of the Controller's response;

5. The basis for the denial of the request if the request is denied in whole or in part; and

6. The existence and resolution of any Consumer appeal to a denied request.

B. Controllers shall maintain a record of all Data Rights requests made pursuant to C.R.S. § 6-1-1306 with which the Controller has previously complied. Such records shall be retained for at least twenty-four (24) months and shall be made available at the completion of a merger, acquisition, bankruptcy, or other transaction in which a Third Party assumes control of Personal Data to ensure any new Controller continues to recognize the Consumer's previously exercised Data Rights.

C. Controllers shall maintain documents sufficient to demonstrate compliance with 4 CCR 904-3, Rules 6.07, 6.08, and 7.06 for as long as the Processing activity continues, and for at least twenty-four (24) months after the conclusion of Processing activity.

D. Required records shall be maintained in a readable format, appropriate to the sophistication and size of the Controller's business.

E. The Controller shall implement and maintain reasonable security procedures and practices, consistent with 4 CCR 904-3, Rule 6.09, in maintaining all required records.

F. Personal Data maintained pursuant to this 4 CCR 904-3, Rule 6.11, where that information is not used for any other purpose, shall not be subject to Data Rights requests.

G. Personal Data maintained for required documentation shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the Colorado Privacy Act, C.R.S. § 6-1-1301, *et seq*., and these rules. Personal Data maintained for required documentation shall not be shared with any Third Party except as

necessary to comply with a legal obligation or as part of a merger, acquisition, bankruptcy, or other transaction in which a Third Party assumes control of Personal Data.

H. Other than as required by this subsection and 4 CCR 904-3, Rule 4.06, a Controller is not required to retain Personal Data solely for the purpose of fulfilling a Data Rights request made under the Colorado Privacy Act, C.R.S. § 6-1-1301, *et seq*.

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 and 6-1-1313. 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), 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.

B. Controllers may rely upon valid consent obtained prior to July 1, 2023, to continue to Process a Consumer's previously collected Personal Data, including Sensitive Data, collected before July 1, 2023. Consent obtained before July 1, 2023, shall be considered valid only if it would comply with the requirements set forth in C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7) and Part 7 of these rules.

1. Controllers that do not obtain valid Consent prior to July 1, 2023 to continue to use, store, or otherwise Process Sensitive Data collected prior to this date must obtain valid Consent, as required by C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7) and Part 7 of these rules, by July 1, 2024 to continue to Process the previously collected Sensitive Data.

2. If a Controller has collected Personal Data prior to July 1, 2023 and the Processing purpose changes after July 1, 2023 such that it is considered a secondary use pursuant to C.R.S. § 6-1-1308(4) and 4 CCR 904-3, Rule 6.08, the Controller must obtain valid Consent, as required by C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7) and Part 7 of these rules, at the time the Processing purpose changes to continue to Process the previously collected Personal Data.

C. Notwithstanding the above, a Controller Processing Sensitive Data Inferences is not required to obtain Consent for the Processing activity if the Processing falls within the requirements of 4 CCR 904-3, Rule 6.10.

Rule 7.03 REQUIREMENTS FOR VALID CONSENT

A. To be valid, a Consent must meet each of the following elements: (1) it must be obtained through the Consumer's clear, affirmative action; (2) it must be freely given by the Consumer; (3) it must be specific; (4) it must be informed; and (5) it must reflect the Consumer's unambiguous agreement.

B. Consent must be obtained through the Consumer's clear, affirmative action. For purposes of obtaining valid Consent:

1. A "clear, affirmative action" means a Consumer's Consent is communicated through either (a) deliberate and clear conduct, or (b) a statement that clearly indicates their acceptance of the proposed Processing of their Personal Data.

2. A blanketed acceptance of general terms and conditions, silence, inactivity or in action, pre-ticked boxes, and other negative option opt-out constructions that require intervention from the Consumer to prevent agreement are not clear affirmative actions for the purposes of valid Consent.

C. Consent must be freely given. For purposes of obtaining valid Consent:

1. Consent is freely given when Consumers may refuse Consent without detriment and withdraw Consent easily at any time.

2. Consent is not freely given when:

a. It reflects acceptance of a general or broad terms of use or similar document that contains descriptions of Personal Data Processing along with other, unrelated information;

b. The performance of a contract is dependent on Consent to Process Personal Data that is not necessary to provide the goods or services contemplated by the contract; or

c. The Controller denies goods, services, discounts, or promotions to a Consumer who chooses not to provide Consent, unless:

i. The Personal Data is necessary to the provision of those goods, services, discounts, or promotions, consistent with 4 CCR 904-3, Rule 6.05; or

ii. The Consent is otherwise required in connection with a Consumer's voluntary participation in a Bona Fide Loyalty Program, consistent with the requirements in 4 CCR 904-3, Rule 6.05.

3. Example: An online dating application's terms and conditions tells users that the application will disclose collected Personal Data, including Sensitive Data revealing sexual orientation, with similar applications for advertising purposes. Consent is required for the disclosure of Sensitive Data with similar applications for advertising purposes. Since users cannot accept the required terms and conditions without the opportunity to

separately provide or withhold Consent for sharing with similar applications, the Consent is not freely given.

D. Consent must be specific.

1. When Controllers request Consent to Process Personal Data for more than one Processing purpose, and those Processing purposes are not reasonably necessary to or compatible with one another, Consumers must have the ability to separately Consent to each specific purpose.

a. Controllers may request Consent to Process Personal Data for multiple Processing purposes that are not reasonably necessary to or compatible with one another using a single Consent request as long there is also an option for more granular Consent within the same Consent interface.

2. Consent to Process Personal Data for one specific purpose does not constitute valid Consent to Process Personal Data for other purposes that are not reasonably necessary to or compatible with that specific purpose.

3. The Sale of Sensitive Data to one specific party is not necessary to or compatible with the Sale of Sensitive Data to a different party.

a. Example: A cosmetic retailer asks a customer for Consent to use Sensitive Data revealing the customer's racial origin in order to provide first-party targeted offers to the customer and to Sell the customer's racial origin information to Data Brokers. This Consent is not specific as there is no opportunity to provide separate Consent for the two separate Processing purposes. Therefore, Consent in this example would not be valid.

b. Example: In the example above, the Controller requests Consent only to Sell Sensitive Data revealing the customer's racial origin with commercial partners. The Controller lists "Fashion Co. #1" and "Make Up Co. #1" as commercial partners who will receive Sensitive Data. Consent would be deemed valid for only these two Third Parties because their identity was provided to the Consumer at the time that his or her Consent was collected. Consent would not be deemed valid for Selling with another Third Party whose identity has not been provided.

E. Consent must be informed.

1. When requesting Consent, a Controller must provide the following information, at a minimum:

a. The Controller's identity;

b. The plain-language reason that Consent is required;

c. The Processing purpose(s) for which Consent is sought;

d. The categories of Personal Data that the Controller shall Process to effectuate the Processing purpose(s);

e. Names of all Third Parties receiving the Sensitive Data through Sale, if applicable;

f. A description of the Consumer's right to withdraw Consent for the identified Processing purpose at any time in accordance with 4 CCR 904-3, Rule 7.07 and details of how and where to do so; and

g. Any disclosures required by 4 CCR 904-3, Rules 6.05 and 9.05.

F. Consent may not be obtained using Dark Patterns as defined in C.R.S § 6-1-1309(9) and prohibited by 4 CCR 904-3, Rule 7.09. Pursuant to C.R.S. § 6-1-1303(5)(c) and 4 CCR 904-3, Rule 7.09, any agreement obtained through Dark Patterns is not valid Consent.

Rule 7.04 REQUESTS FOR CONSENT

A. Controllers shall provide a simple form or mechanism to enable a Consumer to provide Consent when required, including Consent to Processing purposes from which the Consumer has previously opted out. Such a form or mechanism should be easy for a reasonable Consumer to locate and should comply with the other requirements set forth in Part 7 of these rules.

B. Requests for Consent shall be prominent, concise, and separate and distinct from other terms and conditions, and shall comply with all requirements for disclosures and communications to Consumers set forth in 4 CCR 904-3, Rule 3.02.

C. Any Consent request by a Controller must contain the disclosures required by 4 CCR 904-3, Rule 7.03(E)(1) either directly or through a link. Where possible, the request interface itself should contain the disclosures required by 4 CCR 904-3, Rule 7.03(E)(1)(a)-(d). Alternatively, the Controller may provide the Consumer with a link to a webpage containing the required Consent disclosures, provided the request clearly states the title and heading of the webpage section containing the relevant disclosures. If technically feasible, the request method must also link the Consumer directly to the relevant section of the disclosure.

D. Example: A mobile application requests Consent to Process Sensitive Data. The Consent request provides a link to the application's privacy notice which contains the required Consent disclosures. However, the Consent request does not direct or bring the Consumer to the relevant section of the privacy notice. Consent is not valid because the Consent request does not clearly indicate the title and section where the Consumer can find the required disclosures and did not link the Consumer directly to the relevant section of the privacy notice.

E. Example: Acme Toy Store collects customer email addresses in order to send customers information about product recalls, and maintains those email addresses in a recall email distribution list. Acme Toy Store wants to Sell the recall email distribution list to a Third Party partner to enable that partner to send those customers promotional materials. Acme Toy Store must obtain customer consent prior to Selling the recall email distribution list because Selling the recall email distribution list is not reasonably necessary to or compatible with providing product recall information. Acme Toy Store emails its customers attaching a revised privacy notice disclosing the new Processing purpose and asks customers to Consent to the new privacy notice, but does not state the new purpose in the email, and does not direct customers to the section of the privacy notice disclosing the secondary purpose. Consent is not valid because the email did not contain the required Consent disclosures or direct the customers to a document containing the required Consent disclosures.

1. Example: Under the same circumstances, Acme Toy Store emails its customers on the recall distribution list informing those customers that Consent is required for the Acme Toy Store to Process email addresses for the secondary purpose of Selling the recall distribution list to a Third Party partner to enable that partner to send promotional materials, providing all other required disclosures and including a mechanism that enables the customers to provide Consent and to revoke Consent through the same user

interface. Consent is valid because the email contained all required Consent disclosures in an acceptable form.

2. Example: Under the same circumstances, Acme Toy Store emails the product recall email distribution list informing those customers that it would like to use their email addresses for the secondary purpose of Selling the recall distribution list to a Third Party partner as contemplated in section B.2.e. of its privacy notice, explains that it cannot use the customers' email addresses for that secondary purpose without their consent, and requests the customers' Consent to Process their email address for that secondary purpose. It then provides a link directly to section B.2.e. of its privacy notice which explains that Acme Toy Store Sells customer email addresses, including those Processed for the purpose of product recall notifications, to marketing partners, in addition to all other disclosures. The email provides a Consent mechanism that enables the customers to provide or revoke consent through the same user interface. Consent is valid because the email and linked page together contained all required disclosures, the email provided the specific section of the relevant disclosures, and the link brought the customers directly to the relevant disclosures.

Rule 7.05 CONSENT AFTER OPT-OUT

A. The Consumer's decision to Consent to Processing activities from which the Consumer has previously opted-out using either a Universal Opt-Out Mechanism or directly with a particular Controller is subject to the requirements for Consent under 4 CCR 904-3, Rules 7.03 and 7.04.

B. A Controller that wishes to obtain Consent to Process Personal Data for an Opt-Out Purpose after the Consumer has opted out of Processing for that Purpose shall not request Consent using schemes that cause consent fatigue, such as interface dominating cookie banners, high frequency requests, cookie walls, pop-ups, or other any other interstitials that degrade or obstruct the Consumer's experience on the Controller's web page or application.

1. A Controller may proactively request Consent to Process Personal Data for an Opt-Out Purpose after the Consumer has opted out, by providing a link to a privacy settings page, menu, or similar interface, or comparable offline method, that enables the Consumer to Consent to the Controller Processing the Personal Data for the Opt-Out Purpose, so long as the request for Consent meets all other requirements for valid Consent under this Part 7.

2. If a Controller has a reasonable belief that a Consumer intended to opt back into the Sale of Personal Data or Processing of Personal Data for Targeted Advertising, the Controller may proactively send a link to a privacy settings page or other method to enable the Consumer to Consent to the Controller Processing the Personal Data for the Opt-Out Purpose directly to a Consumer.

C. If a Controller conspicuously displays the status of the Consumer's opt-out choice on the website pursuant to 4 CCR 904-3, Rule 5.08(E), the link to provide Consent may appear beside or in conjunction with the Consumer's opt-out status.

D. If a Consumer has opted-out of the Processing of Personal Data for the Opt-Out Purposes, and then initiates a transaction or attempts to use a product or service inconsistent with the request to opt-out, such as signing up for a Bona Fide Loyalty Program that also involves the Sale of Personal Data to a Bona Fide Loyalty Program Partner, the Controller may request the Consumer's Consent to Process the Consumer's Personal Data for that purpose, so long as the request for Consent complies with all provisions of 4 CCR 904-3, Rules 7.03 and 7.04.

E. Example: A Consumer opts out of the use of Personal Data for Sale or Targeted Advertising using a Universal Opt-Out Mechanism. The Consumer visits the website of a fashion retailer that routinely shares Consumer Personal Data for Targeted Advertising. The fashion retailer must obtain the Consumer's consent because the Consumer has already opted out of Processing for that purpose. The fashion retailer's website displays a pop-up banner seeking Consent to share the Consumer's Personal Data for Targeted Advertising. This is not a valid request for Consumer Consent because the request is made through a pop-up banner that degrades or obstructs the Consumer's experience on the Controller's web page or application.

F. Example: A Consumer opts out of the use of Personal Data for Sale or Targeted Advertising using a Universal Opt-Out Mechanism. The Consumer visits a fashion retailer's website. The fashion retailer's homepage contains a message at the top of the webpage that displays the Consumer's opt-out status, stating, "you have opted out of targeted advertising" next to a link that states "Opt-in to Data Use". The linked webpage also meets all requirements of 4 CCR 904-3, Rules 7.03 and 7.04. Consent pursuant to this request is valid.

Rule 7.06 CONSENT FOR CHILDREN

A. When a Controller engages in Processing activities involving the collection and Processing of Personal Data from a known Child or operates a website or business directed to Children or has actual knowledge that it is collecting or maintaining Personal Data from a Child, the Controller must obtain Consent from the parent or lawful guardian of that Child before collecting or Processing the Child's Personal Data.

B. A Controller Processing the Personal Data of a Child must make reasonable efforts to obtain verifiable parental Consent, taking into consideration available technology. Any method to obtain verifiable parental Consent must be reasonably calculated, in light of available technology, to ensure that the person providing Consent is the Child's parent or lawful guardian.

C. Reasonably calculated methods for determining that a person Consenting to the Processing of a Child's Personal Data is the parent or lawful guardian of that Child include, but are not limited to:

1. Providing a Consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;

2. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

3. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

4. Having a parent or guardian connect to trained personnel via videoconference; and

5. Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

D. Any Personal Data collected for purposes of verifying the identity of a parent or legal guardian may not be used for any reason other than Processing these verifications.

Rule 7.07 REFUSING OR WITHDRAWING CONSENT

A. A Consumer shall be able to refuse or revoke Consent as easily and within a similar number of steps as Consent is affirmatively provided.

B. If Consent is obtained through an electronic interface, the Consumer shall be able to refuse or withdraw Consent through the same or similar electronic interface.

C. When using an electronic interface, and when feasible based on the Consumer's relationship with the Controller, a Controller may allow Consumers to track what Processing activities they have Consented to or opted out of.

D. There shall be no detriment to a Consumer for refusing or withdrawing Consent, consistent with C.R.S. § 6-1-1308(1)(c)(II), and 4 CCR 904-3, Rule 6.05.

1. Notwithstanding 4 CCR 904-3 Rule 7.07(D), if a Consumer refuses to Consent to, or withdraws consent for the Processing of Sensitive Data or Personal Data strictly necessary for a program, product or service, the Controller is no longer obligated to provide that program, product or service.

E. If a Consumer withdraws Consent for a Processing activity, subject to Consent under C.R.S. §§ 6-1-1306(1)(a)(IV)(C), 1308(4), and 1308(7), the Controller shall cease that Processing activity and, in the notice required by C.R.S. § 6-1-1306(2), provide the Consumer instructions on how to exercise the right to deletion, provide a link to exercise the right to deletion, or inform the Consumer that information regarding the right to delete their Personal Data can be found in the Controller's privacy notice.

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. § 1308(4), if the Secondary Use involves Profiling for a decision 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.

Rule 7.09 USER INTERFACE DESIGN, CHOICE ARCHITECTURE, AND DARK PATTERNS

A. The following principles should be considered when designing a user interface or a choice architecture used to obtain Consent when required under C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7):

1. Consent choice options should be presented to Consumers in a symmetrical way that does not impose unequal weight or focus on one available choice over another such that a Consumer's ability to consent is impaired or subverted.

a. Example: One choice should not be presented with less prominent size, font, or styling than the other choice. Presenting an "I accept" button in a larger size than the "I do not accept" button would not be considered equal or symmetrical. Presenting an "I do not accept" button in a greyed-out color while the "I accept" button is presented in a bright or obvious color would not be considered equal or symmetrical.

b. Example: If multiple choices are offered to a Consumer, it should be equally easy to accept or reject all options. Presenting the option to "accept all" when offering a Consumer the choice to Consent to the use of Sensitive Data for multiple purposes without an option to "reject all" would not be considered equal or symmetrical.

2. Consent choice options should avoid the use of emotionally manipulative language or visuals to unfairly, fraudulently, or deceptively coerce or steer Consumer choice or Consent.

a. Example: One choice should not be presented in a way that creates unnecessary guilt or shames the user into selecting a specific choice. Presenting the choices "I accept, I want to help endangered species" vs "No, I don't care about animals" may be considered unfairly emotionally manipulative.

b. Example: The explanation of the choice to Consumers should not include gratuitous information to emotionally manipulate Consumers. Explaining that a mobile application "helps save lives" when asking for Consent to collect Sensitive Data for Targeted Advertising may be considered deceptively emotionally manipulative if the Targeted Advertising is not critical to the lifesaving functionality of the application.

3. A Consumer's silence or failure to take an affirmative action should not be interpreted as acceptance or Consent.

a. Example: A Consumer closing a pop-up window which requests Consent without first affirmatively selecting the equivalent of an "I accept" button should not be interpreted as Consent.

b. Example: A Consumer navigating forward on a webpage after a Consent choice has been presented without selecting the equivalent of an "I accept" button should not be interpreted as affirmative Consent.

c. Example: A Consumer continuing to use a Smart TV without replying "I accept" or "I consent" in reply to a verbal request for Consent should not be interpreted as affirmative Consent.

4. Consent choice options should not be presented with a preselected or default option.

a. Example: Checkboxes or radio buttons should not be selected automatically when presented to a Consumer.

5. A Consumer should be able to select either Consent choice option within a similar number of steps. A Consumer's ability to exercise a more privacy-protective option shall not be unduly longer, more difficult, or time-consuming than the path to exercise a less privacy-protective option.

a. Example: Consumers should be presented with all choices at the same time. Presenting an "I accept" button next to a "Learn More" button which requires Consumers to take an extra step before they are given the option of an "I do not accept" button could be considered an unnecessary restriction.

b. Example: Describing the choice before Consumers and placing both the "I accept" and "I do not accept" buttons after a "select preferences" button would not be considered an unnecessary restriction.

6. A Consumer's expected interaction with a website, application, or product should not be unnecessarily interrupted or intruded upon to request Consent.

a. Example: Consumers should not be interrupted multiple times in one visit to a website to Consent if they have declined the Consent choice offered when they arrived at the page.

b. Example: Consumers should not be redirected away from the content or service they are attempting to interact with because they declined the Consent choice offered, unless Consent to process the requested data is strictly necessary to provide the website or application content or experience.

c. Example: Consumers should not be forced to navigate through multiple pop-ups which cover or otherwise disrupt the content or service they are attempting to interact with because they declined the Consent choice offered.

7. Consent choice options should not include misleading statements, omissions, affirmative misstatements, or intentionally confusing language to obtain Consent.

a. Example: Choices should not be driven by a false sense of urgency. A countdown clock displayed next to a Consent choice option which states "time is running out to Consent to this data use and receive a limited discount" where the discount is not actually limited by time or availability would be considered creating a false sense of urgency.

b. Example: Choices should avoid the use of double negatives when describing Consent choice options to Consumers.

c. Example: Consent choice options should not be presented with confusing or unexpected syntax. "Please do not check this box if you wish to Consent to this data use" would be considered confusing syntax.

d. Example: The language used for choice options should logically follow the question presented to the Consumer. Offering the options of "Yes" or "No" to the question "Do you wish to provide or decline Consent for the described purposes" would be considered an illogical choice option. The choice options "provide" and "decline" would be considered to logically follow the same question.

8. The vulnerabilities or unique characteristics of the target audience of a product, service, or website should be considered when deciding how to present Consent choice options.

a. Example: A website or service that primarily interacts with Consumers under the age of 18 should consider the simplicity of the language used to explain the choice options or the way in which cartoon imagery or endorsements might unduly influence their choice.

b. Example: A website or service that primarily interacts with the elderly should consider font size and space between buttons to ensure readability and ease of interaction with design elements.

9. User interface design and Consent choice architecture should operate in a substantially similar manner when accessed through digital accessibility tools.

a. Example: If it takes two clicks for a Consumer to Consent through a website, it should take no more than two actions for a Consumer using a digital accessibility tool to complete the same Consent process.

B. In addition to the principles included in this part 4 CCR 904-3, Rule 7.09(A), Controllers may consider statutes, administrative rules, and administrative guidance concerning Dark Patterns from other jurisdictions when evaluating the appropriateness of the user interface or choice architecture used to obtain required Consent.

C. Controllers shall not use an interface design or choice architecture to obtain required Consent that has been designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making or choice, or unfairly, fraudulently, or deceptively manipulating or coercing a Consumer into providing Consent.

1. The principles outlined in 4 CCR 904-3, Rule 7.09(A) and (B) are factors to be considered when determining if a consent interface design or choice architecture has been designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making or choice, or unfairly, fraudulently, or deceptively manipulating or coercing a Consumer into providing Consent.

D. Consent obtained in violation of this part 4 CCR 904-3, Rule 7.09(C) may be considered a Dark Pattern, as defined in C.R.S. § 6-1-1303(9).

E. The fact that a design or practice is commonly used is not, alone, enough to demonstrate that any particular design or practice is not a Dark Pattern.

F. Consent obtained through Dark Patterns does not constitute valid Consent in compliance with C.R.S. §§ 6-1-1303, 6-1-1306, and 6-1-1308.

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 6-1-1313. 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, 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; 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.

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. § 6-1-1308(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. § 6-1-1309(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.

PART 9 PROFILING

Rule 9.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 9 is C.R.S. §§ 6-1-108(1), 6-1-1302(1)(c)(II)(B), 6-1-1303, 6-1-1306, 6-1-1309, and 6-1-1313. The purpose of the rules in this Part 9 is to provide clarity on the duties and rights related to Profiling.

Rule 9.02 SCOPE

A. Controllers have an affirmative obligation to provide clear, understandable, and transparent information to Consumers about how their Personal Data is used, including for Profiling, pursuant to C.R.S. § 6-1-1302(1)(c)(II)(B).

B. Consumers have the right to opt out of Profiling as defined in C.R.S. § 6-1-1303(20) and 4 CCR 904-3, Rule 2.02 when the Profiling is done in furtherance of a decision 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, pursuant to C.R.S. §§ 6-1-1306(1)(a)(I).

C. Controllers must conduct and document a data protection assessment compliant with C.R.S. § 6-1-1309 and Parts 8 and 9 of these rules before Processing Personal Data for Profiling that presents specific, reasonably foreseeable risks contemplated in C.R.S. § 6-1-1309(2)(a).

Rule 9.03 PROFILING OPT-OUT TRANSPARENCY

A. To ensure that Consumers understand how their Personal Data is used for Profiling in furtherance of Decisions that Produce Legal or Other Similarly Significant Effects Concerning a Consumer, Controllers that Process Personal Data for Profiling for a decision 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 and subject to C.R.S. § 6-1-1306(1)(a)(I) shall provide clear, understandable, and transparent information to Consumers in the required privacy notice, including at a minimum:

1. What decision(s) is (are) subject to Profiling;

2. The categories of Personal Data that were or will be Processed as part of the Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects;

3. A non-technical, plain language explanation of the logic used in the Profiling process;

4. A non-technical, plain language explanation of how Profiling is used in the decision-making process, including the role of human involvement, if any;

5. If the system has been evaluated for accuracy, fairness, or bias, including the impact of the use of Sensitive Data, and the outcome of any such evaluation;

6. The benefits and potential consequences of the decision based on the Profiling; and

7. Information about how a Consumer may exercise the right to opt out of the Processing of Personal Data concerning the Consumer for Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects.

B. Notwithstanding the requirements in 4 CCR 904-3, Rule 9.03(A), nothing in 4 CCR 904-3, Rule 9.03 shall be construed as requiring the Controller to provide information to a Consumer in a manner that would disclose the Controller's trade secrets.

Rule 9.04 OPTING OUT OF PROFILING IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER

A. Consumers have the right to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer through the method specified by the Controller in the required privacy notice, pursuant to C.R.S. § 6-1-1306(1)(a) and 4 CCR 904-3, Rule 4.03.

B. Requests to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer based on Solely Automated Processing or Human Reviewed Automated Processing shall be honored pursuant to C.R.S. § 6-1-1306(2).

C. A Controller may decide not to take action on a request to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer if the Profiling used is based on Human Involved Automated Processing. If a Controller does not take action based on this reason, the Controller shall inform the Consumer pursuant to C.R.S. § 6-1-1306(2)(b) and include the following information, or share a link to such information if it is included in the Controller's privacy notice:

1. The decision subject to the Profiling;

2. The categories of Personal Data that were or will be used as part of the Profiling used in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects;

3. A non-technical, plain language explanation of the logic used in the Profiling process;

4. A non-technical, plain language explanation of the role of meaningful human involvement in Profiling and the decision-making process;

5. How Profiling is used in the decision-making process;

6. The benefits and potential consequences of the decision based on the Profiling; and

7. An explanation of how Consumers can correct or delete the Personal Data used in the Profiling used in the decision-making process.

D. In order to ensure that Consumers have an opportunity to exercise their right to opt out of Profiling in furtherance of Decisions that Produce Legal or Other Similarly Significant Effects Concerning a Consumer, Controllers that Process Personal Data for Profiling covered by C.R.S. §§ 6-1-1303(10) and 6-1-1306(1)(a)(I) shall provide a method to exercise the right to opt out of Profiling in furtherance of Decision that Produce Legal or Other similarly Significant Effects Concerning a Consumer clearly and conspicuously at or before the time such Processing occurs.

E. Notwithstanding the requirements in 4 CCR 904-3, Rule 9.04(C), nothing in 4 CCR 904-3, Rule 9.04 shall be construed as requiring the Controller to provide information to a Consumer in a manner that would disclose the Controller's trade secrets.

Rule 9.05 CONSENT FOR PROFILING IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER

A. When a Consumer has opted out of Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer as defined by C.R.S. § 6-1-1303(10), the Controller may request that a Consumer provide Consent after opting out subject to 4 CCR 904-3, Rule 7.05.

B. If a Controller decides to begin Processing Personal Data for Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer and such Processing is not reasonably necessary to or compatible with the original specified purposes for which the Personal Data was Processed, the Controller shall request the Consumer provide Consent prior to such processing, subject to C.R.S. § 6-1-1308(4) and Part 7 of these rules.

C. Any request for Consent to Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer must include meaningful information about the Profiling that allows a Consumer to make an informed, freely given, and specific choice, including, at a minimum:

1. The decision subject to the Profiling;

2. The categories of Personal Data used in the Profiling;

3. A non-technical, plain language explanation of the logic used in the Profiling, or a link to such information if it is included in the Controller's privacy notice;

4. How Profiling is used in the decision-making process, including the role of human involvement, if any;

5. Why the Profiling is relevant to the decision-making process;

6. Potential benefits and consequences of the decision based on the Profiling; and

7. Any applicable links to where Consumers can find any additional information about the Profiling and decision-making process and their associated rights.

D. Notwithstanding the requirements in 4 CCR 904-3, Rule 9.05(C), nothing in 4 CCR 904-3, Rule 9.05 shall be constructed as requiring the Controller to provide information to a Consumer in a manner that would disclose the Controller's trade secrets.

Rule 9.06 DATA PROTECTION ASSESSMENTS FOR PROFILING

A. Controllers must conduct and document a data protection assessment compliant with C.R.S. § 6-1-1309 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 904-3, 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.

PART 10 ENFORCEMENT

Rule 10.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 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*., and these Colorado Privacy Act Rules, 4 CCR 904-3.

Rule 10.02 ENFORCEMENT CONSIDERATIONS

A. Nothing in the Colorado Privacy Act, C.R.S. § 6-1-1303, *et seq.*, 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 11 MATERIALS INCORPORATED BY REFERENCE

Rule 11.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 10 is C.R.S. §§ 6-1-108(1) and 6-1-1313. The purpose of the rules in this Part 11 is to incorporate by reference the guidelines that are referred to in 4 CCR 904-3, Rule 3.02(A)(2).

Rule 11.02 WEB CONTENT ACCESSIBILITY GUIDELINES

A. The Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, are hereby incorporated into 4 CCR 904-3, Rule 3.02(A)(2) by reference pursuant to C.R.S. § 24-4-103(12.5), and do not include any later amendments.

B. Copies of the Web Content Accessibility Guidelines that are incorporated by reference into these rules may be obtained by sending a written request to the following address by U.S. mail:

Colorado Department of Law
Ralph L. Carr Judicial Center
1300 Broadway, 9th Floor
Denver, CO 80203

C. The Web Content Accessibility Guidelines published by the World Wide Web Consortium incorporated by reference into these rules are available at no cost in an electronic form online at https://www.w3.org/TR/WCAG21/.

D. The Colorado Department of Law also maintains a copy of the Web Content Accessibility Guidelines that are incorporated by reference into these rules that is available for public inspection at the Colorado Department of Law's office during regular business hours.