COLORADO DEPARTMENT OF LAW

Consumer Protection Section

Colorado Privacy Act Rules

4 CCR-904-3

PART 1 GENERAL APPLICABILITY

Rule 1.01 AUTHORITY

The statutory authority for this Part 904-3 is sections C.R.S. §§ 6-1-108(1) and 6-1-1313.

Rule 1.03 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 the Rules shall remain in full force and effect.

PART 2 DEFINITIONS

Rule 2.01 AUTHORITY AND PURPOSE

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.

"**Automated Processing**" as referred to in CRS § 6-1-1303(20) means the Processing of Personal Data that is automated through the use of computers, computer programs or software, or other digital technology.

"**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, including but not limited to a fingerprint, a voiceprint, eye retinas, 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 discounts, rewards, or other actual value to Consumers that voluntarily participate in that program.

"**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.

"**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).

"**Human Involved Automated Processing**" means the Automated Processing of Personal Data where human involvement in the Processing includes meaningful consideration of available data used in the Processing as well as 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 Processing but the level of human review 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 the type of information known to be available to the general public, 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, including but 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. For purposes of this defined term, the term "private parts" includes:

1. Exposed human genitals or pubic area, with less than an opaque covering;

2. A female breast or any portion of the female breast below the top of the areola, with less than an opaque covering;

3. A part of the body that, if revealed publicly, the subject would find sensitive or offensive based on their religious beliefs.

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

''**Publicly Available Information**'' as referred to in C.R.S. § 6-1-1303(17) 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. Inferences made exclusively from multiple independent sources of publicly available information;

3. Biometric Data;

4. Genetic Information;

5. Publicly Available Information that has been combined with non-publicly available Personal Data; or

6. 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 geolocation information at a high level may not be considered Sensitive Data, geolocation data which shows an individual visited a mosque and is used to indicate that individual's religious beliefs is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a). Similarly, geolocation data which shows an individual visited a reproductive health clinic and is used to indicate 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, creates a profile that indicates an individual's sexual orientation and 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 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 pursuant to C.R.S. § 6-1-1313(2).

PART 3 CONSUMER DISCLOSURES

Rule 3.01

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 are able to 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 to Consumers pursuant to 4 CCR 904, Rules 3-4.02, 5.03, 6.01, 6.05, and 7.04 must be:

1. 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 903-3-10.02. In other contexts, the Controller shall provide information on how a Consumer with a Disability may access the disclosure or communication 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 an interface regularly used in conjunction with the Controller's product or service.

5. Readable on all devices through which Consumers interact with the Controller, including on smaller screens and through mobile applications, if applicable.

6. Unless otherwise stated, notifications from Controllers to Consumers shall be communicated in a manner by which the Controller regularly interacts with Consumers.

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. Any method specified by a Controller must comply with each of the following:

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

a. A Controller that operates 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 (A)(1)(a), above, 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. Comply with requirements provided in 4 CCR 904-3, Rule 3.01;

3. 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;

4. Be easy for Consumers to execute, requiring a minimal number of steps; and

5. Not use Dark Patterns, as defined by C.R.S. § 6-1-1303(9) and prohibited by 4 CCR 904-3, Rule 7.09.

B. 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.

C. 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.

D. 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.

E. If a Consumer or Authorized Agent submits a request for an Opt-Out Purpose in a manner that is not one of the Controller's specified Data Rights request methods, or the request 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 with information on how to submit the request or remedy any deficiencies in the request.

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, but no later than fifteen (15) days from the date the Controller receives the request.

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

B. A Controller must provide an opt-out method, either directly or through a link, clearly and conspicuously in its privacy notice as well as in a clear, conspicuous, and readily accessible location outside the privacy notice.

1. 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," or "Your Opt-Out Rights."

2. The opt-out method must:

a. Comply with 4 CCR 904-3, Rule 4.02.

b. Describe the Consumer's right to opt out and provide instructions on how to opt out.

3. The clear, conspicuous, and readily accessible location must be:

a. Positioned in an obvious location of a website or application, such as the header or footer of a Controller's internet homepage, or an application's app store page or download page; and

b. Available to the Consumer at or before the time the Personal Data is Processed for the Opt-Out Purposes.

C. An Authorized Agent may exercise a Consumer's opt-out right, so long as the Authorized Agent's request permits the Controller to Authenticate the identity of the Consumer and the Authorized Agent's authority to act on the Consumer's behalf.

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, including without limitation, any Personal Data that the Controller's Processors obtained in providing services to the Controller.

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

1. Understandable to the Controller's target audiences, considering vulnerabilities or unique characteristics of the audience and paying particular attention to vulnerabilities of Children.

2. Provided in the language in which the Consumer interacts with the Controller.

3. Provided in a form that would allow the average Consumer to make an informed decision of whether to exercise deletion, correction, or opt-out rights.

a. For instance, the Personal Data must be provided in a form that is concise, transparent and easily intelligible, and avoids incomprehensible or unexplained internal codes and identifiers.

b. Nothing herein shall prevent a Controller from complying fully with a Consumer's data portability request pursuant to C.R.S. § 6-1-1306(1)(e).

C. 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, or Biometric Data. 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.

Rule 4.05 RIGHT TO CORRECTION

A. A Controller shall comply with a Consumer's correction request by correcting the Consumer's Personal Data across all data flows and repositories and implementing measures to ensure that the Personal Data remains corrected. The Controller shall also instruct all Processors that maintain the Personal Data at issue to make the necessary corrections in their respective systems and to ensure that the Personal Data remains corrected.

B. 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 3.01;

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.

C. A Controller 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 based on the totality of the circumstances.

1. 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. 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.

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 in accordance with C.R.S. § 6-1-1303(11); and

2. Notifying the Controller's Processors and Affiliates to delete the Consumer's Personal Data obtained from the Controller.

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 for a Sale, disclosure, or commercial purpose.

D. If a Consumer submits a deletion request with respect to Personal Data that falls within an exception under C.R.S. § 6-1-1304, the Controller shall delete the Consumer's Personal Data that is not subject to the exception; provide the Consumer with a list of Personal Data that was not deleted along with the applicable exception; and not use the Consumer's Personal Data retained for any other purpose than provided for by the applicable exception.

E. 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.

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 enables the Consumer to have complete access to and full enjoyment of the Personal Data, including, but not limited to, the capacity to save, edit, and transfer the Personal Data to any other person or platform at Consumer's discretion.

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.

1. Notwithstanding 4 CCR 904-3, Rule 4.07(B), Personal Data or Sensitive Data Inferences created using a trade secret algorithm or other mechanism must be disclosed to comply with a data portability request without disclosing the algorithm or mechanism itself.

Rule 4.08 AUTHENTICATION

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

B. When possible, a Controller shall avoid requesting additional Personal Data to Authenticate a Consumer unless the Controller cannot Authenticate the Consumer from 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 or to Authenticate an Authorized Agent's authority, 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.

D. A Controller shall implement reasonable security measures, consistent with 4 CCR 904-3, Rule 6.90, 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 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. If a Controller decides not to act on a Consumer's Data Right request, the Controller's response to the Consumer must include the basis for the Controller's decision, including but not limited to (1) any conflict with federal or state law; (2) the relevant exception to the Colorado Privacy Act; (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 good-faith, documented belief that the request is fraudulent or abusive.

1. If a Controller has a good-faith claim that complying with the Consumer's request would be impossible, the Controller must explain in its response, in detail, why compliance is impossible.

2. If a Controller has a good-faith, documented belief that a request is fraudulent or abusive, the Controller must explain in its response why it believes the request is fraudulent or abusive.

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

4. 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).

C. When a Controller complies with a Consumer's Personal Data Right request, the Controller shall also notify all Processors that Process the Consumer's Personal Data of the Consumer's request and the Controller's response.

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

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 rule 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.

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 express a Consumer's choice to opt out of the Processing of Personal Data for all purposes subject to the opt-out right or it may express a Consumer's choice to opt out of the Processing of Personal Data for one specific purpose only. A Universal Opt-Out Mechanism may offer "all purposes" or "specific purposes" options, or both.

Rule 5.03 NOTICE AND CHOICE

A. The platform, developer, or provider that provides a Universal Opt-Out Mechanism shall make clear to the Consumer, whether in its configuration or disclosures to the public, that the mechanism is meant to have the effect of opting the Consumer out of the Processing of Personal Data for specific purposes or all 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 3.01;

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

3. Shall clearly describe the mechanism's limitations, including, for example:

a. Whether the mechanism will have the effect of opting the Consumer out of the Processing of Personal Data for only one specific Processing purpose; or

b. Whether the mechanism is unable to opt the Consumer out of Processing through mobile or other applications.

4. Shall not use Dark Patterns as defined in C.R.S. § 6-1-1303(9) and prohibited by 4 CCR 904-3, Rule 7.09; and

5. Need not be tailored only to Colorado or refer to Colorado.

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).

Rule 5.04 DEFAULT SETTINGS

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 send 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 say "yes" and enable the signal 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 prominently as a privacy-protective tool or specifically as a tool designed to exercise a user's rights to opt out of the Processing of Personal Data shall be considered the Consumer's affirmative, freely given, and unambiguous choice to use a Universal Opt-Out Mechanism.

1. Example: A browser manufacturer markets its browser as a "privacy friendly" browser, 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.

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 confirm a Consumer is a resident of Colorado or 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).

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.

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.

2. The Universal Opt-Out Mechanism may operate through a means other than by sending an opt-out signal, for example by maintaining a "do not sell" list, so long as Controllers are able to query such a list in an automated manner.

C. 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.

2. The Universal Opt-Out Mechanism may allow a Consumer to opt out of one or more Controllers that recognize the mechanism, to opt out of one or more domain, or to opt out of Processing by all Controllers that recognize the mechanism.

D. 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.

E. 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.

F. A Universal Opt-Out Mechanism must not unfairly disadvantage any Controller. For example, a Universal Opt-Out Mechanism may not treat different Controllers differently or 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 April 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 this section;

2. Be an open system or standard, which 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; and

3. 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 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.

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, 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 browser, device, or Consumer overrides the opt-out, as specified in 4 CCR 904-3, Rule 5.10.

B. A Controller shall be capable of recognizing any Universal Opt-Out Mechanism recognized under subsection 4 CCR § 904-3, Rule 5.07. For example, in the case of a recognized Universal Opt-Out Mechanism sent as a signal, the Controller must listen for the signal. In the case of a recognized Universal Opt-Out Mechanism utilizing a "do not sell" list, the Controller must query the "do not sell" list.

C. A Controller may also recognize Universal Opt-Out Mechanisms that are not recognized under subsection 4 CCR § 904-3, Rule 5.07.

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 the Universal Opt-Out Mechanism.

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.

Rule 5.9 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 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 contains all information required in 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 3.01.

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.

2. 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 the following information for each Processing purpose:

   a. The Processing purpose described in a level of detail that gives Consumers a meaningful understanding of how their Personal Data is used and why their Personal Data is reasonably necessary for the Processing purpose.

   b. If the Processing purpose includes Targeted Advertising or Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer, the Controller shall list that activity as part of the Processing purpose.

   c. The categories of Personal Data Processed for each of the Controller's Processing purposes, including, but not limited to, whether Sensitive Data or the Personal Data of a Child is Processed. 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: "real name," "contact information," "government issued identification numbers," "payment information", "Information from Cookies," "data revealing religious affiliation," and "medical data."

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

   e. Categories of Third Parties to whom the Controller sells, or with whom the Controller shares Personal Data, if any, for each Processing purpose. Categories of Third Parties must be described in a level of detail that gives Consumers a meaningful understanding of what type of entity the Third Party is, and to the extent possible, how the Third Party may Process Personal Data.

      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." For each processing purpose, whether the Personal Data collected is Sold or processed for Targeted Advertising.

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), 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 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 twelve (12) 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 substantive or material changes to a privacy notice, including, but not limited to, changes to: (1) categories of Personal Data Processed; (2) Processing purposes; (3) a Controller's identity; or (4) methods by which Consumers can exercise their Data Rights request. Changes to a privacy notice shall be communicated to Consumers in a manner by which the Controller regularly interacts with Consumers.

B. Notice of a substantive or material change to a privacy notice must be made 15 calendar days before the change goes into effect.

C. A Controller must obtain Consent from a Consumer pursuant to 4 CCR 904-3, Rules 7.02-7.05 before Processing Personal Data for a secondary use, even if the new purpose is disclosed in the privacy notice.

Rule 6.05 LOYALTY PROGRAMS

A. While a Controller may not increase the cost of or decrease the availability of a product or service based solely on a Consumer's exercise of a Data Right, a Controller is not prohibited from offering Bona Fide Loyalty Program Benefits to a Consumer based on the Consumer's voluntary participation in that 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 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.

D. 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 3.01 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 E., below.

E. 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 as required by 4 CCR 904-3, Rule 6.05(E), as well as in its privacy notice, Bona Fide Loyalty Program terms, and Consent disclosures in requests for Consent to Process Sensitive Data or Personal Data in connection with the Bona Fide Loyalty Program:

    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, including whether Personal Data will be provided to Data Brokers;

    c. The value of the Bona Fide Loyalty Program Benefits available to the Consumer if the Consumer opts out of the Sale of Personal Data or Processing of Personal Data for Targeted Advertising, and the value of the Bona Fide Loyalty Program Benefits available to the Consumer if the Consumer does not opt out of the Sale of Personal Data or Processing for Targeted Advertising; and

    d. A list of any Bona Fide Loyalty Program Benefits that require the Processing of Personal Data for Sale or Targeted Advertising, and the Third Party receiving the Personal Data and providing each such Bona Fide Loyalty Program Benefit, if applicable.

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.

F. Example: A Consumer joins a pharmacy's Bona Fide Loyalty Program that includes both personalized and non-personalized Bona Fide Loyalty Program Benefits. The pharmacy asks the Consumer for Consent to collect Sensitive Data about the Consumer's prescriptions and medical conditions 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 pharmacy 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.

Rule 6.06 PURPOSE SPECIFICATION

A. Controllers shall specify the express purposes for which Personal Data are collected and Processed in both external disclosures to Consumers as well as in any internal documentation required by this Part 6.

B. The express purpose must be described in a sufficiently unambiguous, specific, and clear manner, such that the way Personal Data will be Processed is understood by and predictable to the average Consumer, the Controller, Third Parties, and enforcement authorities.

1. Particular care should be taken to ensure that any specification of the purpose is sufficiently clear to all involved, irrespective of their different cultural or linguistic backgrounds, level of understanding, or special needs.

2. The express purpose must be detailed enough to enable the implementation of necessary data security safeguards and allow for compliance with the law to be assessed.

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 avoid identifying one broad purpose to justify numerous Processing activities that are only remotely related.

2. Controllers should avoid specifying one broad purpose to cover potential future Processing activities that are only remotely related.

D. If the Processing purpose has evolved beyond 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. Such assessment shall be documented according to 4 CCR 904-3, Rule 6.11.

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.

2. Biometric Identifiers 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. Controllers must obtain Consent to Process Biometric

Identifiers or any Personal Data generated from a digital or physical photograph or an audio or video recording each year after the first year that it is stored.

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 before the time the Personal Data is collected 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), the Controller must obtain Consent pursuant to C.R.S. § 6-1-1308 and 4 CCR 904-3, Rules 7.02-7.05.

C. If a new Processing purpose is unexpected, unnecessary, unconnected, or would have an unjustified negative impact on the Consumer, the new purpose is not likely to be considered reasonably necessary to or compatible with the original specified purpose. When considering if the new Processing purpose is reasonably necessary to or compatible with the original specified purpose, Controllers should 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 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, an Affiliate, a Processor, or a Third Party; and

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

D. An assessment of the reasonable necessity or compatibility of any new Processing purpose shall be documented consistent with 4 CCR 904-3, Rule 6.11.

Rule 6.09 DUTY OF CARE

A. Personal Data must be Processed in a manner that ensures appropriate security and confidentiality of the Personal Data, including protection 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, using reasonable technical or organizational measures.

B. Reasonable measures to secure Personal Data include but are not limited to those provided by C.R.S. § 6-1-713.5 and C.R.S. § 24-73-102.

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 Process Sensitive Data Inferences from Consumers over the age of thirteen (13) without Consent 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. The Personal Data and any Sensitive Data Inferences are permanently deleted within twelve (12) hours of collection or of the completion of the Processing activity, whichever comes first;

3. The Personal Data and any 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 twelve (12) 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 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 a record of any analysis of 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 three (3) years 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, § 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, § 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 these rules in this Part 7 is to provide clarity on the requirements to obtain Consent, 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. If a Controller has collected Sensitive Data prior to July 1, 2023 and has not also previously obtained valid consent to Process such Sensitive Data, the Controller shall obtain consent as required by January 1, 2023 to continue to Process the Sensitive 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. Consumers may refuse Consent without detriment and withdraw Consent easily at any time.

2. Consent is not freely given when:

a. It is bundled with other terms and conditions;

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 asks users for information about their sexual orientation to provide a more targeted service. The application's terms and conditions also tell users that the application will share the collected Personal Data with similar applications for advertising purposes. Consent is required because Personal Data revealing sexual orientation is Sensitive Data. 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 unrelated or incompatible Processing purpose, Consumers must have the ability to separately Consent to each specific purpose.

2. Consent to Process Personal Data for one purpose does not constitute valid Consent to Process Personal Data for other purposes.

3. Consent to Sell or share Sensitive Data or Personal Data with certain parties does not constitute valid Consent to Sell or share Sensitive Data or Personal Data, when required, with other parties.

4. Example: A cosmetic retailer asks a customer for Consent to use Sensitive Data revealing the customer's racial origin in order to provide targeted offers to the customer and to share the customer's racial origin information with commercial partners. 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.

5. Example: In the example above, the Controller requests Consent only to share 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 sharing with another Third Party whose identity has not been provided.

E. Consent must be informed.

1. A request for Consent must contain the following disclosures:

a. The Controller's identity;

b. The reason that Consent is required;

c. The Processing purpose for which Consent is sought;

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

e. Categories of all parties who will have access to the Personal Data, and names of all Third Parties and Affiliates receiving the Sensitive Data through Sale or sharing. Names of Processors, as defined in C.R.S. § 6-1-1306(19) are not required; and

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.

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 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 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 3.01.

C. A Consent request method may provide the Consumer with a link to a webpage containing the Consent disclosures required by 4 CCR 904-3, Rule 7.03, provided the request method clearly states the title and section of 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 collect health information to provide diet and fitness advice. 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 use the recall email distribution list to send those customers promotional materials. Acme Toy Store must obtain customer consent prior to using the recall email distribution list to provide promotional materials because providing promotional materials is not necessary to or compatible with providing product recall information. Acme Toy Store emails the recall distribution list attaching a revised privacy notice disclosing the new promotional purposes 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 the recall email distribution list informing those customers that Consent is required for the Acme Toy Store to Process email addresses for a secondary purpose, explaining that the secondary purpose is to provide customers with 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 a secondary purpose as contemplated in section B.2.e. of its privacy notice and requests the customers' Consent to do so. It then provides a link directly to section B.2.e. of its privacy notice which explains that Acme Toy Store uses customer email addresses to send information about Acme Toy Store's sales and promotions, 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. If a Controller wishes to proactively obtain Consent to Process Personal Data for an Opt-Out Purpose after the Consumer has opted out of Processing for that Purpose, a Controller shall provide a link or similar mechanism on its website or application that enables the Consumer to provide Consent. The link or similar mechanism must:

1. Have a similar look, feel, and size relative to other links on the same web page or application, and not be presented through pop-up windows, pop-up banners, or other web interface displays that degrade or obstruct the Consumer's experience on the Controller's web page or application; and

2. Meet all other requirements for a valid Consent under this Part 7.

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, 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 states "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. If a Controller 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 shall take commercially reasonable steps to verify a Consumer's age before Processing that Consumer's Personal Data.

B. When a Controller engages in Processing activities involving the collection and Processing of Personal Data from a known Child, the Controller must obtain Consent from the parent or lawful guardian of that Child before collecting or Processing the Child's Personal Data.

C. 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.

D. 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.

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.

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

F. Parental verification and Consent pursuant to this section must be documented as required by 4 CCR 904-3, Rule 6.11.

Rule 7.07 REFUSING OR WITHDRAWING CONSENT

A. A Consumer shall be able to refuse or revoke Consent as easily and within the same 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 electronic interface.

C. When using an electronic interface and when feasible based on the Consumer's relationship with the Controller, a Controller should 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.

E. If a Consumer withdraws Consent for a Processing activity, the Controller shall cease that Processing activity and provide the Consumer instructions on how to exercise the Right to Deletion or provide a link to exercise the Right to Deletion.

1. If the Personal Data subject to the withdrawal of Consent is Sensitive Data, the Controller shall, pursuant to C.R.S. § 6-1-1308(3) and 4 CCR 904-3, Rule 6.07, delete or otherwise render permanently anonymized or inaccessible the Sensitive Data collected solely for the purpose of that Processing activity and not reasonably necessary in relation to another specified purpose for which the Controller has obtained and continues to have valid Consent.

Rule 7.08 REFRESHING CONSENT

A. A Controller that has obtained Consent from a Consumer must refresh Consent in compliance with all requirements of this Part 7 at regular intervals based on the context and scope of the original Consent, sensitivity of the Personal Data collected, and reasonable expectations of the Consumer.

B. 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.

C. For Processing of Sensitive Data, Consent must be refreshed at least annually.

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

A. Controllers shall not use an interface design or choice architecture that has 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.

B. The following principles shall be considered when designing a user interface or a choice architecture:

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.

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 coerce or steer Consumer choice.

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” could be considered 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 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 radial buttons should not be selected automatically when presented to a Consumer.

5. A Consumer should be able to select either Consent choice option within the same number of steps.

   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.

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.

C. The use of Dark Patterns, as defined in C.R.S. § 6-1-1303(9), is prohibited.

D. Consent obtained in violation of this part 4 CCR 904-3, Rule 7.09 may be considered a Dark Pattern. Any agreement 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.

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. In addition to the principles included in this part 4 CCR 904-3, Rule 7.09, Controllers may consider statutes, administrative rules, and administrative guidance concerning Dark Patterns from other jurisdictions when evaluating the appropriateness of their proposed choice architecture or system design.

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 that: 1) identifies and describes all risks posed by Processing that presents a heightened risk of harm to a Consumer; 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.

C. The depth, level of detail, and scope of data protection assessments should be proportionate to the size of the Controller, amount and sensitivity of Personal Data Processed, and Personal Data Processing activities subject to the assessment.

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 Processing operations using similar methods to collect the same categories of Personal Data for the same purposes.

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 should involve all relevant internal actors from across the Controller's organizational structure, and where needed, 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 describe each of the following:

1. The Processing activity;

2. The specific purpose of the Processing activity;

3. The specific types of Personal Data to be Processed as well as the sources and amount of Personal Data collected, how long the Personal Data will be maintained, and whether it includes Sensitive Data, including Personal Data from a known Child as described in C.R.S. § 6-1-1303(24);

4. How the Personal Data to be Processed is adequate, relevant, and limited to what is reasonably necessary in relation to the specified purpose;

5. Operational details for the Processing, including planned processes for Personal Data collection, use, storage, retention, and sharing, and the technology or Processors to be used;

6. Names and categories of Personal Data recipients, including Third Parties, Affiliates, and Processors that will have access to the Personal Data;

7. The relationship between the Controller and the Consumer(s) whose Personal Data will be Processed;

8. The expectations of the Consumer(s) concerning how their Personal Data will be used, including expectations based on privacy notices, Consent disclosures and unique vulnerabilities;

9. Procedural safeguards to be afforded to the Consumer when Personal Data is obtained, including:

    a. Whether and how the Controller will request Consent, if required, in accordance with Part 7 of these rules;

    b. Whether and how the Controller will provide Consumers the opportunity to opt out of Processing, if required, in accordance with 4 CCR 904-3, Rule 4.03 and Part 5 of these rules; and

    c. Whether and how the Controller will review web interfaces to be used in Consent requests for Dark Patterns.

10. Alternative Processing activities considered to achieve the same purpose;

11. The sources and nature of risks to individual Consumers and broader Consumer groups 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. Issues that a Controller may consider in a data protection assessment include, for example:

    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, privacy 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.

12. Measures and safeguards a Controller will put into place to mitigate risks and comply with C.R.S. § 6-1-1308, which may include, but are not limited to:

a. Measures to secure Personal Data during storage, use, and transfer, including any relevant data security frameworks used;

b. Measures to limit the categories and amount of Personal Data to be Processed;

c. The use of De-identified Data;

d. Measures taken to prevent the Processing activity from leading to unlawful discrimination;

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

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

13. 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;

14. 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 twelve (12) hours of the Personal Data Processing activity subject to the exception, as well as the auditing procedure for this process;

15. The benefits of the Processing that may flow to the Controller, Consumer, and other expected stakeholders, and how the benefits outweigh the risks, as mitigated by safeguards, and justify the Processing activity;

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

17. The data protection assessment review process, including whether any internal or external audit was conducted, and if so, the name of the auditor, the names and positions of individuals involved in the review process, and the details of the audit process; and

18. 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 data 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 periodically 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 conducted after July 1, 2023 and are 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), 6-1-1306, 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 when the Profiling is done in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer, 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 Part 8 of these rules before Processing Personal Data for Profiling as contemplated in C.R.S. §§ 6-1-1303(10) and 6-1-1309(1)(a)(I).

D. The Automated Processing used in Profiling includes Solely Automated Processing, Human Reviewed Automated Processing, and Human Involved Automated Processing, as defined at 4 CCR 904-3, Rule 2.02.

Rule 9.03 PROFILING OPT-OUT TRANSPARENCY

A. To ensure that Consumers understand how their Personal Data may be 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 covered by C.R.S. §§ 6-1-1303(10) and 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 is 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 plain language explanation of the logic used in the Profiling process;

4. Why Profiling is relevant to the ultimate decision;

5. If the Profiling is used to serve ads related to housing, employment, or financial or lending services;

6. 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;

7. The benefits and potential consequences of the decision concerning the Consumer; and

8. 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) 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 not 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:

1. The decision subject to the Profiling;

2. The specific pieces of Personal Data that were or will be used as part of the Profiling used in the decision-making process;

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

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

5. Why the Profiling is relevant to 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 in any required privacy notice and in a clear, conspicuous, and readily accessible location outside of the privacy notice.

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 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 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 if the decision is based on Solely Automated Processing, Human Reviewed Automated Processing, or Human Involved Automated Processing;

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. A link 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 9.03 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. Rules 8.01-8.05 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 includes Profiling using Solely Automated Processing, Human Reviewed Automated Processing, and Human Involved Automated Processing.

C. "Unfair or deceptive treatment" as used in this 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 this 4 CCR 904-3, Rule 9.06 includes conduct or activity which violates state or federal laws that prohibit unlawful discrimination against Consumers.

E. "Other substantial injury" to Consumers as used in this 4 CCR 904-3, Rule 9.06 includes but is not limited to a small harm to a large number of Consumers.

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:

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 the automated decision-making system;

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;

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 of the accuracy and reliability of the software;

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.

PART 10 MATERIALS INCORPORATED BY REFERENCE

Rule 10.01 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 10 is to incorporate by reference the guidelines that are referred to in 4 CCR 904-3, Rule 3.01(A)(2).

Rule 10.02 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 3.01(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.

Notice of Proposed Rulemaking
Department of Law
Attorney General - Consumer Protection Section
Colorado Privacy Act Rules
4 CCR 904-3

Date & Time of Public Hearings
Wednesday, February 1, 2023, at 10:00 AM MST

I. Notice

As required by the Colorado Administrative Procedure Act found at C.R.S. § 24-4-103, the Department of Law gives notice of proposed rulemaking in connection with draft rules governing the implementation of the Colorado Privacy Act, C.R.S. § 6-1-1301, *et seq*. ("CPA").

The proposed rulemaking hearing is scheduled for February 1, 2023, at 10:00 AM, and will continue as needed. The hearing will be conducted both in person and by video conference. All interested parties must register to attend the public hearing through the registration link provided in the table below.

Date	Location	Time	Registration Link
February 1, 2023	In Person: Office of The Attorney General Colorado Department of Law Ralph L. Carr Judicial Building 1300 Broadway, Room 1D Denver, CO 80203 Video Conference: Link available upon registration	10:00 AM	https://us02web.zoom.us/webinar/register/WN_FjjpF9kMQ_aKBoC1rGI6KQ

How to Register for the Rulemaking Hearing
You must click on the registration link provided in the table above to register for the hearing. When you register, you must provide your full name and email address. You may also provide the name of the organization that you are representing, if any. Finally, please indicate whether you plan on attending the hearing in person or remotely by video conference, and whether you plan to testify during the hearing. When you submit your registration, you will receive a confirmation email including details about how to join the hearing virtually or attend in person. The registration link for the hearing is also available on the Colorado Department of Law's CPA rulemaking website at coag.gov/CPA.

II. Subject

The Colorado Department of Law (the "Department") is considering rules governing the implementation of the CPA. The specific purpose of this rulemaking is to create rules governing the ways in which the CPA shall be carried out, including the clarification of Consumer Data Rights, Controller Obligations, and technical specifications for one or more Universal Opt-Out Mechanisms.[1]

Only the rule provisions included in the proposed draft rules will be opened for comment during this rulemaking period. A detailed Statement of Basis, Purpose, and Specific Statutory Authority and the complete set of proposed draft rules follow this notice and are incorporated herein by reference.

The Department invites comments from all members of the public regarding the proposed draft rules during the rulemaking process. Additionally, the Department welcomes input responsive to the following specific questions. Please note that these questions are not intended to limit input or indicate that the Department is predisposed to any position or action.

1. Definitions (4 CCR 904-3, Rules 2.01, et seq.)

- *Biometric Data.* The CPA does not define Biometric Data. The Department based the proposed definition of "biometric data" on corresponding laws in the United States. Does this definition sufficiently capture and protect biometric information?
- *Widely Available Information.* The CPA does not define or use the phrase "Widely Available Information" in its definition of "Publicly Available Information." The Department has clarified the scope of "information that a Controller has a reasonable basis to believe the Consumer has lawfully made available to the general public" to address concerns raised during the pre-rulemaking period. Are there any other examples that can be provided to further refine this proposed definition?
- *Publicly Available Information.* The Department has provided clarity regarding information that is not included in the proposed definition of "Publicly Available Information." Of note, Personal Data obtained or processed in violation of C.R.S. §§ 18-7-107 and 18-7-801 have been excluded from the definition of "Publicly Available Information." Are there any other laws that should be included? Are there additional exclusions beyond these laws the Department should include?

2. Consumer Personal Data Rights (4 CCR 904-3, Rules 4.01, et seq.)

- *Right to opt out*. The CPA requires that Controllers provide an opt-out method "clearly and conspicuously in any privacy notice required to be provided to Consumers under this part 13, and in a clear, conspicuous, and readily accessible location outside the privacy notice."

[1] All undefined terms capitalized herein shall be interpreted as defined in the CPA or proposed Rules

What does "conspicuous and readily accessible location" mean with respect to Controllers that do not have a direct relationship with Consumers? Is a location on a Controller's website conspicuous and readily accessible if a Consumer has no way to know that the Controller is Processing that Consumer's Personal Data?

- *Right of access*. The CPA provides Consumers with the right to access the Consumer's Personal Data that is maintained or otherwise Processed by a Controller. How should a Controller provide Personal Data to a Consumer in response to an access request? Is there a particular form that would best enable a Consumer to make an informed decision of whether to exercise deletion, correction, or opt-out rights?
- *Right to correction.* The draft rules anticipate instances where Personal Data may be corrected more quickly and easily through account settings than through the Data Rights request process at 4 CCR 904-3, Rule 4.05(B). Does the language provided in this rule sufficiently effectuate this point? How might the language be modified to deter Controllers from abusing the purpose of the provision?
    - When the Consumer and the Controller disagree on the accuracy of the Personal Data in question, the draft rules include a provision allowing a Controller to request documents supporting the Consumer's assertion that the Personal Data is incorrect before completing the request. Does this provision provide adequate instruction to address the issue? Is there a way to establish the accuracy of Personal Data that would be less burdensome on Consumers?
- *Authentication.* The draft rules instruct Controllers on the CPA's requirements for Authenticating a Consumer or authorized agent submitting a Data Rights request. Do these Authentication requirements sufficiently contemplate data security and protection against identity theft? When and why should a Controller be able to deny a Consumer's Data Rights Request based on inability to Authenticate? Are there additional factors that we should consider with respect to Authentication of Authorized Agents?
- *Appeal process*. Does the CPA sufficiently address the process of appealing a Controller's actions in response to a Consumer Data Rights request? Would additional rules be helpful? What parts of the appeals process could benefit from interpretive guidance or description of best practices?

3. Universal Opt-Out Mechanism (4 CCR 904-3, Rules 5.01, et seq.)

- *Offline Recognition.* Are Controllers who interact with Consumers offline, such as through in-person interactions, able to recognize the use of Opt-Out Mechanisms? What additional Personal Data would be required to enable offline recognition?
- *Universal Opt-Out Mechanism List.* The draft rules explain that the Department will maintain a public list of Universal Opt-Out Mechanisms to simplify the options facing Controllers, Consumers, and other actors. Will this list lessen the compliance burden? Are there sources for similar lists? How might this aid

interoperability with other jurisdictions with similar Universal Opt-Out provisions? How often should this list be updated?

- *Universal Opt-Out Mechanism Standards.* The draft rules include standards that a Universal Opt-Out Mechanism must meet to be included in the public list maintained by the Department. Are these the most important considerations? What additional considerations should we include in the list of standards?
- *Notice.* The draft rules allow for a Controller to display to a Consumer that it has Processed the Consumer's opt-out preference signal via a Universal Opt-Out Mechanism, for example through conspicuous text on its website. What kind of engineering or business resources would be required for a Controller to display this kind of notice? How might it benefit Consumers?
- *Timing.* The draft rules state that a "public list of Universal Opt-Out Mechanisms that have been recognized...shall be released no later than April 1, 2024." Will this date offer Controllers sufficient time to implement the acceptance of recognized Universal Opt-Out Mechanisms by the July 1, 2024 effective date of the relevant provision statute (C.R.S. § 6-1-1306(1)(a)(IV)(B))? What burdens are associated with the July 1, 2024 compliance deadline? If the list is updated, how long should Controllers have prior to mandated acceptance of new mechanisms?
- *Technical Specification.* The draft rules contemplate Universal Opt-Out Mechanisms taking two technical forms: a signal such as an HTTP header field and a "do not sell" list. Should the final rules spell out these two forms? Are there other forms the rules should mention? Are there additional areas of technical specification that would help further clarify the parameters or requirements of a Universal Opt-out Mechanism.
- *Authentication*. The CPA provides that the rules must "permit the Controller to accurately Authenticate the Consumer as a resident of this state and determine that the mechanism represents a legitimate request to opt out of the Processing of Personal Data for purposes of Targeted Advertising or the Sale of Personal Data. . . ." What are ways for a Controller to Authenticate a Consumer as a resident of this state and to determine that the mechanism represents a legitimate request to opt out in a way that would not frustrate the efficiency or purpose of using a Universal Opt-Out Mechanism?

4. Controller Obligations (4 CCR 904-3, Rules 6.01, et seq.)

- *Transparency*. The draft rules require Controllers to provide information "for each Processing purpose." Will organizing a privacy notice by purpose place an undue burden on Controllers? What can be changed to ensure these requirements are interoperable while providing the same amount of valuable information to Consumers?
- *Changes to Privacy Notice*. Are there additional examples of material changes to privacy notices that would help to clarify the requirement to notify Consumers of "substantial or material changes"?
- *Biological Identifiers.* The draft rules limit the storage of "Biological Identifiers or any data generated from a digital or physical photograph or an audio or video

recording" and require Consent to continue to hold such information for more than 1 year. Does this rule sufficiently protect this type of data? How might this requirement burden Controllers?

- *Sensitive data*. The draft rules explain that Sensitive Data includes Sensitive Data Inferences. The draft rules allow Controllers to process Sensitive Data Inferences from Consumers over the age of thirteen (13) without obtaining Consent subject to specific requirements in the draft rules, including the requirement to delete the Sensitive Data Inferences "within twelve (12) hours of collection or of the completion of the Processing activity, whichever comes first." What burden might this 12-hour deletion requirement create? Are the requirements related to Sensitive Data Inferences sufficient to protect Consumers? How might the rules further promote data minimization with regard to Sensitive Data?

5. Bona Fide Loyalty Programs (4 CCR 904-3, Rule 6.05)

- *Definition*. The CPA expressly allows Controllers to offer benefits to Consumers if the benefits are based on a Consumer's participation in a "bona fide loyalty, rewards, premium features, discount, or club card program," but does not define "bona fide" in the loyalty program context. Does the proposed definition of "Bona Fide Loyalty Program" provide sufficient clarity as to when the CPA's loyalty program provisions apply? Are there additional factors that should be considered in determining whether a loyalty program is bona fide?
- *Value*. What actual value can a loyalty program provide to consumers? To Controllers? What are important considerations when balancing the value of a loyalty program to Consumers versus Controllers? When and why is the Sale of Personal Data necessary to maintain a loyalty program or provide loyalty program benefits?
- *Disclosures*. Are there different or additional disclosures that should be made to Consumers concerning Bona Fide Loyalty Programs?
- *Guidance*. Are there aspects of the loyalty program statutory provisions or draft rules that can benefit from more guidance?

6. Consent (4 CCR 904-3, Rules 7.01, et seq.)

- *Consent Elements.* In response to public input, the draft rules provide the meaning of each element of valid Consent. Are the elements described in a way that would be interoperable? Are there additional examples that would help clarify the meaning of any element of Consent? Are there other factors pertaining to any of the elements that should be considered when determining whether Consent is valid?
- *Examples.* Do the examples provided help to clarify the Consent requirements? Is there anything unclear in the Consent examples? Are there other elements of Consent where additional examples would be helpful?

7. Data Protection Assessments (DPAs) (4 CCR 904-3, Rules 8.01, et seq.)

- *Purpose.* The draft rules focus, in part, on making DPAs meaningful assessments that can help Controllers understand and address the risks posed by their Processing activities and address those risks. Do the draft rules achieve this purpose? If not, how can they be changed to avoid making the DPA process a "check-the-box" exercise?
- *Burden.* Are the DPA requirements expressed in the draft rules overly burdensome on smaller businesses? How so? How can they be made less burdensome?

8. Profiling (4 CCR 904-3, Rules 9.01, et seq.)

- *Automated Processing.* The draft rules distinguish between Solely Automated Processing, Human Reviewed Automated Processing, and Human Involved Automated Processing. Do these distinctions appropriately reflect different levels of human participation in the Automated Processing used in Profiling? How else might humans be involved with Automated Processing which would protect Consumers when such Profiling is used for Decisions that Produce Legal or Similarly Significant Effect?
- *Human Involved Automated Processing*. The draft rules specify disclosures that a Controller must provide to a Consumer if the Controller does not take action on a request to opt out of Profiling when that Profiling uses Human Involved Automated Processing. Are there additional disclosures that would provide Consumers with adequate information to understand this use of their data?

9. Clarity

- Are there draft rules that are unclear? Where would examples provide additional clarity? Beyond examples, how else might the Department help clarify the rules?
- Are there examples used in the draft rules that are unclear?

III. Statutory Authority

The specific authority under which the Attorney General shall establish these proposed rules is set forth in C.R.S. §§ 6-1-108(1) and 6-1-1313.

IV. Copies of the Notice, Proposed Rules, and the Statement of Basis, Purpose & Authority

The notice of hearing, the proposed rules, and the Statement of Basis, Purpose, and Specific Statutory Authority are available for review at the Department of Law's CPA rulemaking website at coag.gov/CPA. If there are changes made to the proposed rules prior to the hearing, the updated proposed rules will be provided to the CPA rulemaking mailing list and posted on the Department of Law's website by January 25, 2023. The Department encourages all interested parties to sign up for the Colorado Privacy Act rulemaking mailing list (available at https://lp.constantcontactpages.com/su/zIKnX1I/CPA).

Please note that the proposed rules being considered are subject to further changes and modifications after the public hearings and the deadline for the submission of written comments.

V. Opportunity to Testify and Submit Written and Oral Comments

The Attorney General and Department of Law strive to make the rulemaking process inclusive to all. Interested and affected parties are welcome to testify at the rulemaking hearing, to submit written comments through the online CPA rulemaking comment portal, and to provide oral comments at one or more stakeholder meetings.

Rulemaking Hearing (Wednesday, February 1, 2023)

The format of the rulemaking hearing will proceed as follows:

- The Hearing Officer will open the hearing and provide a brief introduction of the hearing procedures.
- The Colorado Department of Law staff will present the draft rules and discuss public input, feedback, and suggestions on the draft rules provided through written comment and at stakeholder sessions.
- Colorado Department of Law staff will present a summary of the draft rules and any proposed revisions based on rulemaking comments.
- Participants will then have the opportunity to give testimony regarding the proposed rules and revisions.

Hybrid Hearing Procedures

At the beginning of the hearing, we will mute all public participants attending online. After the introduction, a summary of the rulemaking, and a review of any proposed revisions to the rules, we will open the hearing to testimony as follows:

- For the sake of efficiency, those who are attending this hearing in person will be called upon first to provide their public comment. We will reference the sign-up sheet provided and individually call upon participants who wish to provide their testimony. Once we have exhausted the sign-up sheet, we will move forward with the testimony of online participants.
- Referencing registration records, we will identify and individually unmute online participants who indicated that they plan to testify during the hearing.
- When we exhaust the list, we will ask whether any additional attendees wish to testify. In-person attendees may raise their hands to indicate their intention to testify, and online attendees may raise/lower their hand virtually.
- To ensure that the hearing is prompt and efficient, oral testimony may be time limited.

Webinar Audio Requirements: We strongly encourage attendees to join the webinar through their computer or Zoom meeting app, even if they use their telephone to dial in for audio. To testify during the hearing, it is best to use your computer microphone and speakers or a headset or headphones. As outlined above, we will first receive online

testimony from attendees whose registration indicates that they plan to provide testimony and then we will offer attendees the option to raise their hand to testify.

Written Comments

You may submit written comments through our comment portal available at coag.gov/CPA during the comment period between October 10, 2022, and February 1, 2023. If the formal rulemaking hearing continues beyond February 1, 2023, the comment period will continue through the last day of the formal rulemaking hearing. Please submit written comments by November 7, 2022, if you would like your comment to inform the stakeholder meetings discussed below, or by January 18, 2023, to be considered for any proposed revisions presented at the hearing. All written comments must be received on or before Wednesday, February 1, at 11:59 P.M. MST, or if the formal rulemaking hearing continues beyond February 1, 2023, before 11:59 P.M. MST on the last day of the formal rulemaking hearing.

As soon as possible after receipt, written comments will be posted online at the Colorado Privacy Act Rulemaking Comment website: https://comments.coag.gov/s/. All written comments will be added to the official rulemaking record.

To promote timely sharing of information among all stakeholders, the Department strongly encourages stakeholders to submit written comments early in this process.

Stakeholder Meetings

The Department will host three (3) virtual stakeholder meetings to discuss the CPA proposed draft rules. These stakeholder meetings are a forum for the Department to gather feedback from a broad range of stakeholders for the development of rules to implement the CPA. Stakeholder meetings will occur in advance of the rulemaking hearing and speaking participants will be asked to provide their input and insight, along with constructive feedback and suggestions, on the draft rules in an open discussion format. Please submit any written comments you would like to inform these stakeholder meetings by Monday, November 7, 2022.

The Department may host additional opportunities for public input beyond those listed below if it determines doing so is prudent or necessary to revise the rules and incorporate stakeholder input. The times and dates of these additional sessions will be announced via the Colorado Privacy Act rulemaking mailing list and on our website at coag.gov/CPA. Interested persons are strongly encouraged to sign-up to receive e-mail updates through the rulemaking mailing list (available at https://lp.constantcontactpages.com/su/zIKnX1I/CPA).

Meeting Dates

Date: Thursday, November 10, 2022
Topics: Consumer Rights and Universal Opt-Out Mechanisms

Date: Tuesday, November 15, 2022
Topics: Controller Obligations and Data Protection Assessments

Date: Thursday, November 17, 2022
Topics: Profiling, Consent, and Definitions

All stakeholder meetings will be recorded, and the recordings will be available to interested persons unable to attend a meeting. Recordings will also be part of the public rulemaking record. More details on the stakeholder meetings and registration links can be found on the Department of Law's CPA rulemaking website at coag.gov/CPA.

VI. Recording of the Hearing

The hearing will be recorded. Both the hearing and recordings will be part of the public rulemaking record. After the hearing concludes, the recording will be available on the Colorado Department of Law's CPA Rulemaking website at coag.gov/CPA.

VII. Special Accommodations

If you need special accommodations, please contact our office at coprivacy@coag.gov at least two (2) weeks prior to the scheduled hearing date.

COLORADO DEPARTMENT OF LAW
Colorado Privacy Act Rules
Statement of Basis, Specific Statutory Authority, and Purpose

4 CCR 904-3

Basis

On July 7, 2021, Governor Polis signed Senate Bill 21-190: Protect Personal Data Privacy, establishing the Colorado Privacy Act, C.R.S. §§ 6-1-1301, *et seq*. ("CPA"). The Colorado Privacy Act Rules ("CPA Rules" or "Rules") implement and enforce the CPA.[1]

The Attorney General's Specific Statutory Authority

The CPA was codified as part of the Colorado Consumer Protection Act ("CCPA"), which grants the Attorney General the authority to "promulgate such Rules as may be necessary to administer the provisions" of the CCPA. C.R.S. § 6-1-108(1). The CPA gives the Attorney General authority to "promulgate Rules for the purpose of carrying out" the CPA, C.R.S. § 6-1-1313(1), 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 . . ." C.R.S. § 6-1-1313(2).

Purpose of the Rules

The proposed draft Rules were written by the Colorado Department of Law Consumer Protection Section (the "Department") to help Colorado Consumers understand their data privacy rights under the CPA and to create straightforward processes which enable them to exercise those rights. The proposed draft Rules also aim to clarify the obligations that businesses, public entities, and nonprofits have under the CPA and to facilitate their compliance.

Coloradans have a fundamental right to privacy that is enshrined in article II, section 7 of the Colorado Constitution. However, evolving technology and the exponential increase in the collection and exchange of Personal Data threatens Coloradans' ability to meaningfully exercise their right to privacy. Additionally, while data science has produced beneficial new technologies and insights, the misuse of Consumer Personal Data can cause substantial economic, physical, emotional, and reputational harm to Colorado Consumers.

The CPA protects Coloradans' privacy in part by granting them rights to access the data that companies have collected about them, as well as to dictate whether and how companies can continue to collect, store, use, or sell Consumer Personal Data. However, the CPA does not place the sole burden on Consumers to safeguard their data. It also requires companies to be transparent about how they use Personal Data and to take precautions to reduce the risk that their data collection and use might pose to Consumers. Finally, the CPA grants the Attorney General the authority not only to hold entities accountable for failing to

[1] All undefined terms capitalized herein shall be interpreted as defined in the CPA or proposed draft Rules.

comply with their obligations under the CPA, but also to draft Rules that would clarify the CPA's requirements and provide guidance for compliance.

The specific subject matter of this Rulemaking falls into two discrete categories: Rules detailing the technical specifications for one or more Universal Opt-Out Mechanisms and Rules for the purpose of carrying out the CPA.

The CPA requires compliance and permits enforcement starting July 1, 2023. Accordingly, the Department filed its notice of proposed Rulemaking on October 10, 2022, to ensure the Rules are adopted well in advance of enforcement. This timeframe also provides additional time to both collect and incorporate meaningful stakeholder input on the proposed draft Rules and to give covered entities advanced notice of the Rules so they may take appropriate measures to comply with the CPA and its Rules by the CPA's effective date.

The promulgation of these proposed draft Rules does not preclude any Rulemaking the Attorney General chooses to conduct at a later date pursuant to C.R.S. §§ 6-1-108(1) or 6-1-1313.

Rulemaking Considerations

Public involvement and transparency are important to the success of the CPA rulemaking process. The proposed draft Rules incorporate and reflect public input received from a wide variety of interested parties, including Consumer privacy advocates, representatives from businesses entities, academics, and the public. The Department plans to further engage with stakeholders and interested parties to gain valuable insight and comments and refine the proposed draft Rules. Additional details on opportunities for public participation in the rulemaking process and a list of specific questions and considerations for public comment can be found in the Notice of Proposed Rulemaking and on the Department's CPA Rulemaking website at www.coag.gov/cpa.

Before writing the proposed draft Rules, the Department solicited input to understand how regulations could best clarify the CPA, protect Consumers, and enable compliance. Starting in February of 2022, members of the public and other interested parties were given the opportunity to provide written and oral comments about the CPA to the Department. To guide this process, the Department released "Pre-Rulemaking Considerations for the Colorado Privacy Act," a document containing background information and a list of questions about the Colorado Privacy Act and Consumer data privacy[2]. From March through August of 2022, the Department accepted written comments through an online portal. Additionally, the Department held two public listening sessions on June 22, 2022, and June 28, 2022. Pre-Rulemaking comments and recordings of the public listening sessions can be found on the Department's CPA website[3]. Throughout this process, individual members of the Department met with interested persons to discuss topics relevant to the CPA and the Department began assembling a list of persons interested in the prospective Rulemaking.

[2] Colorado Department of Law, Pre-Rulemaking Considerations for the Colorado Privacy Act, available at https://coag.gov/app/uploads/2022/04/Pre-Rulemaking-Considerations-for-the-Colorado-Privacy-Act.pdf.
[3] Colorado Attorney General's Office, Colorado Privacy Act (CPA) Rulemaking, http://caog.gov/cpa

In creating the proposed draft Rules, the Department considered the questions, concerns, suggestions, and resources shared by interested parties. The Department also reviewed relevant academic research and existing regulations governing overlapping conduct in U.S. and international privacy laws. In considering this input, the Department sought to address the questions and concerns of the variety of CPA stakeholders, clarify the legislation, simplify compliance, and ensure the protection of the privacy rights granted to Consumers by the CPA. The Department also endeavored to create a legal framework that can operate in conjunction with other national, state, and international data privacy laws and does not overly burden technological innovation.

Considerations for specific draft Rules are outlined below.

A. Part 2: Definitions/Defined Terms

Draft Rule 904-3-2.02 defines key terms used in the CPA and the draft Rules and incorporates definitions in the CPA to provide clarity and consistency. In particular, draft Rule 904-3-2.02 defines "Biometric Data" and "Bona Fide Loyalty Program," which were undefined by the statute, and clarifies scope of Automated Processing, Sensitive Data, and Publicly Available Information governed by the statute and draft Rules. Defining these and other terms will help eliminate potential misunderstandings or confusion, and where possible, align the CPA with corresponding laws across the United States and internationally. Clear definitions also assist businesses in implementing the law and its corresponding Rules, increasing the likelihood that Consumers will enjoy the benefits of the rights provided to them by the CPA.

B. Part 4: Consumer Personal Data Rights

Part 4 of the proposed draft Rules clarifies the Consumer Personal Data Rights provided by the CPA. The purpose of these draft Rules is to ensure that Consumers can exercise those Data Rights securely and without undue burden, while considering compliance costs by emphasizing interoperability with other privacy regimes. The draft Rules also clarify obligations for Controllers to collect and use Personal Data responsibly and in a way that respects Consumer preferences. The proposed draft Rules aim to carry out the CPA by clarifying these rights and obligations and providing clear processes through which they can be exercised.

The CPA states that "Consumers may exercise the [data] rights by submitting a request using the methods specified by the Controller," but provides little guidance as to what a Controller's rights request methods must look like and what a Controller must do to comply with such requests. C.R.S. § 6-1-1306(1). Draft Rule 904-3-4.02 details requirements for methods through which Consumers may submit Data Rights requests. In designing these methods, a Controller must consider several factors to determine the suitability of the methods, including how the Controller typically interacts with Consumers, identifiable security risks, and the ease of use for Consumers with varying abilities. The draft Rule clarifies restrictions on the type of information a Controller can collect from a Consumer seeking to exercise a Data Right and how a Controller may respond to deficient Data Rights requests.

Draft Rule 904-3-4.03 elaborates on C.R.S. § 6-1-1306(1)(a), which establishes a Consumer's right to opt out of the Processing of their Personal Data and Controllers' related compliance requirements. The draft Rule emphasizes the need for clear instructions to the Consumer, ease of exercising the opt-out right, and prompt response from the Controller. To promote interoperability and decrease compliance costs, the draft Rule articulates that Controllers who already provide an opt-out method pursuant to another privacy regime may continue to use that method for Colorado Consumers if the method meets the requirements under the draft Rule.

Draft Rule 904-3-4.04 contemplates the right to access as described in C.R.S. § 6-1-1306(1)(b). The draft Rule clarifies the way a Controller must respond to a Consumer's access right request, requiring Controllers to consider the Consumers' primary languages and accessibility needs when providing a Consumer access to their Personal Data. The draft Rule also accounts for risks of identity theft, security, and scams.

Draft Rule 904-3-4.05 clarifies the Consumer right in C.R.S. § 6-1-1306(1)(c) to "correct inaccuracies in the Consumer's Personal Data." The draft Rule provides that Controllers must pass down Consumers' correction requests across all Processor data flows. The draft Rule also seeks to ensure data accuracy by allowing Controllers to consider all available information indicative of accuracy, including documentation provided by the Consumer, and promotes secure communication between Consumers and Controllers when contemplating the data's accuracy.

Draft Rule 904-3-4.06 clarifies the Consumer right in C.R.S. § 6-1-1306(1)(d), to "delete Personal Data concerning the Consumer," ensuring meaningful compliance with Consumer deletion rights requests. Based on public input and considering interoperability with the privacy legislation of other states, the draft Rules also address effective compliance with the right to delete by business-to-business companies that collect Consumer Personal Data from third-party sources on an ongoing, repetitive basis.

Draft Rule 904-3-4.07 clarifies the Consumer right to data portability expressed in C.R.S. § 6-1-1306(1)(e), ensuring that the Personal Data transferred pursuant to that right is both secure and usable by the Consumer. The Rule also addresses the trade secret protection contemplated in C.R.S. § 6-1-1306(1)(e), by distinguishing between a Controller's duty to provide Personal Data and inferences created using trade secrets and the Controller's ability to protect the trade secrets themselves.

Draft Rules 904-3-4.08 - 4.09 address Controller obligations to respond to Consumer rights requests as stated in C.R.S. § 6-1-1306(2). The draft Rules provide clarity while balancing Controllers' need for flexibility when designing Consumer authentication processes and potential burdens on Consumers.

C. Part 5: Universal Opt-Out Mechanism

Part 5 of the draft Rules fulfills the Attorney General's Rulemaking obligation to promulgate a Rule that addresses the technical specifications of one or more Universal Opt-Out Mechanisms (UOOM).

Rather than require Consumers to opt out of Processing on only a case-by-case basis, the CPA gives Consumers the ability to use a UOOM to communicate their opt-out choice to multiple Controllers using a single, simple technological mechanism. The CPA charges the Attorney General with establishing the technical specifications with which UOOMs must comply to qualify under the CPA.

Draft Rule 904-3-5.06 provides the basic technical specification. It is written in a technologically neutral manner, able to accommodate different approaches to providing UOOM capability and leaving room for innovation and competition. It recognizes that a common method for providing UOOM-like functionality has been by sending an "opt-out signal." The language describing universal opt-out signals as UOOMs will aid interoperability, as other jurisdictions speak specifically about signal-based mechanisms. At the same time, the draft Rules leave open the possibility for other technical solutions. It lists a universal opt-out "whitelist" as one example, albeit one meant to be illustrative rather than limitative.

Draft Rule 904-3-5.02 clarifies that a single UOOM can be used by a single Consumer to opt-out of more than one type of Processing as allowed under the CPA.

Draft Rule 904-3-5.03 focuses on the obligations of the "platform, developer, or provider" who proposes, creates, and markets new UOOMs. Companies that provide UOOMs, such as browser manufacturers or browser plug-in developers, must take steps to ensure that the design of their UOOM satisfies all of the CPA's requirements for UOOMs. For example, UOOMs must be designed without Dark Patterns, to ensure that Consumers do not enable UOOMs unintentionally.

Draft Rule 904-3-5.04 clarifies the CPA's requirement that UOOMs must not adopt a mechanism that is a default setting. It gives detailed examples of commonly encountered situations to help elaborate what counts as a default setting in these circumstances.

During the pre-rulemaking phase, commenters raised the potential problems that might rise from the proliferation of many competing UOOMs. Without some method to single out which UOOMs must be recognized under the CPA, Controllers would be obligated to monitor all UOOMs, an expensive and time-consuming task. Consumers might also be confused by the proliferation of many UOOMs and lack clarity on which UOOMs would be accepted by different Controllers. To address this concern, draft Rule 904-3-5.07 sets out a system of recognition through which the Department will maintain a public list of UOOMs. These rules seek to allow for innovation and account for technical advancements in privacy and UOOMs while minimizing redundant UOOMs and UOOMs that are no longer used commercially. Then, under draft Rule 904-3-5.08, Controllers will be obligated to recognize all UOOMs on the public list.

The other draft Rules in this part cover the information gathered in the UOOM process (draft Rule 904-3-5.05) and consent after use of a UOOM (draft Rule 904-3-5.09).

D. Part 6: Duties of Controllers

Part 6 elaborates on the duties of Controllers as stated in C.R.S. § 6-1-1308. The draft Rules respect the need for interoperability while adhering to the legislator's intent and statutory text of the CPA. The draft Rules also seek to allow for creativity and innovation by Controllers while providing sufficient Consumer protection.

The CPA creates obligations for entities that process and sell a large volume of Consumer Personal Data and that either conduct business in Colorado or target their products and services towards Colorado. Generally, these entities must only collect Personal Data they need and must use reasonable practices to secure it.

The CPA aims to help Consumers understand how their Personal Data is being used and how they can exercise their rights. Draft Rules 904-3-6.02 - 6.04 clarify the requirements in C.R.S. § 6-1-1308(1) for Controllers to "provide Consumers with a reasonably accessible, clear, and meaningful privacy notice . . ." Controllers must disclose in a privacy notice the purposes for which they Process Personal Data, and for each purpose, the types of Personal Data they collect, process and share, and the categories of parties with whom they share that Personal Data. The draft Rules contemplate a purpose-based approach in an attempt to help provide Consumers with an accurate expectation of the ways in which their Personal Data will be used. For instance, Consumers will know whether contact information collected for one purpose will be used differently than contact information collected for a different purpose, and can therefore make more informed decisions about how they would like to interact with covered businesses.

Furthermore, Controllers must inform Consumers of how they can access, correct, delete, and download and transmit their Personal Data. This includes notifying Consumers that their Personal Data is being Sold or used for Targeted Advertising or certain types of Profiling, and how Consumers can opt-out. The draft Rule elaborates on these requirements while considering businesses' needs for interoperable standards among state and international frameworks and Consumers' need to easily locate information relevant to understanding how their Personal Data is collected and used.

Draft Rule 904-3-6.05 clarifies the text in C.R.S. § 6-1-1308(1)(d), explaining that the CPA does not prevent Controllers from "offering a different privacy, rate, level, quality, or selection of goods or services to a Consumer, including offering goods or services for no fee, if the offer is related to a Consumer's voluntary participation in a bona fide loyalty, rewards, premium, features, discount, or club card program." Loyalty programs can provide real value to Consumers in the form of discounts on essential goods, rewards towards travel and other services that increase quality of life. The draft Rules seek to facilitate continuation of these programs and while providing greater transparency and meaningful consent to participation.

Draft Rules 904-3-6.06 - 6.09 clarify the Controller duties of purpose specification, data minimization, secondary use, and care found in C.R.S. § 6-1-1308(2)-(5). These draft Rules explain how each statutory requirement is to be carried out to help ensure the intended positive impact on Consumer privacy and offer compliance guidance.

Draft Rule 904-3-6.06 relates to the Controller's duty to "specify the express purposes for which Personal Data are collected and processed" found at C.R.S. § 6-1-1308(2). The draft Rule requires Controllers to describe Processing purposes in ways that are easily understood

to Consumers, across the Controller's business, by Third Parties, and by authorities. The draft Rule also requires regular review of Processing purposes for accuracy and appropriate documentation.

Draft Rule 904-3-6.07 clarifies the requirement in C.R.S. § 6-1-1308(3) for Controllers' "collection of Personal Data [to] be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed." The draft Rule articulates that Controllers must assess and document the minimum types and amount of Personal Data needed for the stated Processing purposes. The draft Rule also clarifies standards to govern how long certain types of Personal Data may be held and requires Controllers to only store the minimum Personal Data necessary for the Processing purpose.

Draft Rule 904-3-6.08 clarifies the prohibition in C.R.S. § 6-1-1308(4) to "process Personal Data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the Personal Data are processed, unless the Controller first obtains the Consumer's consent." The draft Rule clarifies that the specified purpose may be disclosed in several places including a privacy notice and required consent disclosures. To aid in compliance, the draft Rule lists several considerations for the Controller to consider when determining whether a new purpose is reasonably necessary to or compatible with the original purpose.

Draft Rule 904-3-6.09 clarifies the requirement in C.R.S. § 6-1-1308(5) to "take reasonable measures to secure Personal Data during both storage and use from unauthorized acquisition." The draft Rule aligns this requirement with existing state data security laws including but not limited to C.R.S. §§ 6-1-713.5 and 24-73-102.

Draft Rules 904-3-2.01 and 904-3-6.10 clarify the CPA's Sensitive Data requirements at C.R.S. § 6-1-1308(7). The draft Rules state that Sensitive Data includes both individual pieces of Sensitive Data and inferences made by a Controller which reveal 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. However, a Controller may forgo obtaining Consent prior to Processing Sensitive Data Inferences from Consumers over the age of thirteen (13) if the Controller limits the use of such inferences as set forth in Rule 904-3-6.10 and documents how the Controller meets the requirements in its privacy notice and Data Protection Assessment. These draft Rules address the concern that Personal Data can often be combined or used to infer sensitive information, often without a Consumer's knowledge or understanding. At the same time, the draft Rules recognize the potential burden of requiring prior Consent to process every Sensitive Data Inference and seeks to strike a balance that will protect sensitive Consumer information and offer adequate transparency without unduly burdening Controllers.

E. Part 7: Consent

Part 7 of the draft Rules clarifies the CPA's requirements related to requesting and obtaining Consent, including the prohibition against obtaining Consumer agreement through

Dark Patterns, which are understood to be web or user interfaces that have the effect of subverting user autonomy, decision making, or choice.

Because the Consent requirements are provided in separate sections of the CPA, draft Rule 904-3-7.02 provides a straightforward list of the circumstances under which the CPA requires Consumer Consent pursuant to C.R.S. §§ 6-1-1303(5), 1306(1)(a)(IV)(C), 1308(4), and 1308(7). The draft Rule also clarifies the need for valid Consent across distinct Controller-Consumer interactions.

Draft Rule 904-3-7.03 clarifies the requirements for valid Consent in C.R.S. § 6-1-1303, including what it means for Consent to be "freely given, specific, informed, and [reflect] unambiguous agreement." This draft Rule was written in response to public input requesting additional information on the requirements for valid Consent, and it attempts to promote interoperability and understanding by incorporating the meanings of "freely given, specific, informed," and "unambiguous agreement" accepted in other jurisdictions applying similar requirements for valid Consent.

Draft Rule 904-3-7.05 clarifies C.R.S. § 6-1-1306(1)(a)(IV)(C), which states in part that "a Controller may enable the Consumer to Consent, through a web page, application, or a similar method, to the Processing of the Consumer's Personal Data for the purposes of Targeted Advertising or Sale, and the Consent takes precedence over any choice reflected through the universal opt-out mechanism." The CPA gives Consumers the right to make a meaningful choice to opt out of the Sale or Processing of their Personal Data for Targeted Advertising and Profiling. It also enables Consumers to effectuate that choice easily using a Universal Opt-Out Mechanism. A Consumer's decision to opt-out is eroded if Controllers repeatedly ask for a Consumer to opt back into Processing using methods that degrade or obstruct the Consumer's experience on the Controller's web page or application. Thus, the draft Rule sets forth a framework for Controllers to request, and for Consumers to provide, Consent to opt in to Processing of Personal Data once the Consumer has already opted out of the Processing for the stated purpose.

Draft Rule 904-3-7.06 clarifies the requirements to obtain Consent with respect to Children's Personal Data under C.R.S. § 6-1-1308(7). Permission to process the Personal Data of a Child is dependent on the Consent of the Child's parent or guardian. The draft Rule requires Controllers to make reasonable efforts to obtain verifiable parental Consent, taking into consideration available technology.

Draft Rules 904-3-7.07 and 904-3-7.08 also clarify the ability of Consumers to withdraw Consent and ability of Controllers to periodically refresh Consent. The draft Rules address statutory text, common practice, and the meaning of "freely given Consent" to emphasize that a Consumer must be able to withdraw Consent as easily as it is affirmatively provided, to explain what that means, and to describe required actions that a Controller must take when Consent is withdrawn.

Draft Rule 904-3-7.09 clarifies C.R.S. § 6-1-1303(5)(c), which states that an "agreement obtained through Dark Patterns" does not constitute Consent. C.R.S. § 6-1-1303(9) defines a Dark Pattern as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice." The

draft Rule seeks to align the definition of Dark Patterns with existing legal standards by prohibiting Controllers from using an interface design or choice architecture that unfairly, fraudulently, or deceptively manipulates or coerces a Consumer into providing Consent. To show the types of practices that Dark Patterns may encompass, the draft Rule includes examples of established Dark Patterns,[4] including distracting pop-up windows, nagging, misleading questions, emotional manipulation, nested options, and other models that use default options, give greater weight to one option over others through interface design, or allow the absence of a Consumer's action to constitute consent. The draft Rule also requires Controllers to consider the unique characteristics of their target audiences when designing Consent request interfaces and states that a design or practice can be a Dark Pattern even if such a design or practice is commonly used.

F. Part 8: Data Protection Assessments

Part 8 of the draft Rules clarifies the CPA's data protection assessment ("DPA") requirements pursuant to C.R.S. § 6-1-1309. The draft Rules considers stakeholder input received during the pre-Rulemaking phase by addressing the need for interoperable standards and meaningful assessments.

The CPA requires Controllers to prepare and document DPAs before engaging in Processing activities that present a heightened risk of harm to Consumers. Activities that present heightened risks include profiling activities that present a foreseeable risk of unfairness, injury, or an offensive intrusion of consumer privacy; selling Personal Data or using Personal Data for Targeted Advertising; or Processing Sensitive Data.

Draft Rules 904-3-8.02 - 8.05 encourage Controllers to conduct a genuine, thoughtful analysis in their DPAs. To promote communication and encourage involvement by internal stakeholders, the draft Rules require Controllers to involve all relevant internal parties in the analysis, and to include external parties if helpful in identifying and assessing risks to Consumers. The draft Rules list the minimum content requirements for a DPA and suggest risks that should be considered in the assessment process. Controllers need to conduct an initial DPA before beginning the Processing in question and then regularly review the DPA throughout the Processing lifecycle to ensure that existing safeguards adequately control the Processing risks and are adjusted as necessary.

To promote interoperability, the draft Rules allow Controllers conducting similar assessments pursuant to other privacy regimes to use those assessments to meet their CPA compliance requirements if the assessments are reasonably similar in scope and effect.

G. Part 9: Profiling

Part 9 of the draft Rules clarifies the requirements on Controllers that Process Personal Data for the purposes of Profiling pursuant to C.R.S. §§ 6-1-1302, 1306, and 1309.

---

[4] *See e.g.* Jamie Luguri and Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 Journal of Legal Analysis 43 (2021), https://doi.org/10.1093/jla/laaa006; Jennifer King and Adriana Stephan, *Regulating Dark Patterns in Practice: Drawing Inspirations from California Privacy Rights Act*, 5 Georgetown Law and Technology Review 250 (2021); Johanna Gunawan, et al, *A Comparative Study of Dark Patterns Across Web and Mobile Modalities*. Proc. ACM Hum.-Comput. Interact. 5, CSCW2, Article 377 (October 2021), https://doi.org/10.1145/3479521.

The CPA includes several requirements for Profiling activities. Controllers have an affirmative obligation to tell Consumers how their Personal Data is used, including for Profiling. Controllers must also conduct and document DPAs prior to Processing Personal Data for Profiling. Finally, Consumers have the right to opt out of the Processing of Personal Data for the purpose of Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects. Draft Rules 904-3-9.03 - 904-3-9.06 clarify these requirements and their implications. Profiling is unique to other types of Processing activities because it involves automation and large data sets. Research has shown that Automated Processing for the purposing of Profiling poses significant risk without meaningful human intervention, especially when used to provide services that dictate individuals' access to essential programs and services such as education, financial services, and housing.[5] Without human review or intervention, Automated Processing may discriminate or wrongly deny individual Consumers access to these services. The draft Rules delineate between Automated Processing involving different levels of human involvement, as increased human involvement may offer corresponding levels of Consumer protection.

To guard against adverse outcomes in the most sensitive and important areas of a person's life, draft Rule 904-3-9.04 clarifies a Consumer's right to opt out of Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer. The draft Rule supports the CPA's goals of providing transparent information to Consumers about how their Personal Data is used by outlining disclosure requirements for Automated Processing.

H. Other Rules

Finally, while the Department has endeavored to make this Statement of Basis, Specific Statutory Authority, and Purpose comprehensive, the details contained herein may not fully delineate the issues that are discussed or the Rules that are eventually adopted. The Department intends to take stakeholder input sincerely, and this may result in additional Rules, significant changes to the proposed draft Rules, or additional portions of Rules that are not detailed herein. For this reason, the Department strongly encourages all

[5] *See e.g.* Marco Almada, *Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems*, Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law, June 2019, https://dl.acm.org/doi/abs/10.1145/3322640.3326699; Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, Science, Oct. 25, 2019, https://science.sciencemag.org/content/366/6464/447; Madalina Busuioc, *Accountable artificial intelligence: Holding algorithms to account*, 81.5 Public Administration Review 825 (2021), https://onlinelibrary.wiley.com/doi/full/10.1111/puar.13293; Maria De-Arteaga, Riccardo Fogliato, and Alexandra Chouldechova, *A Case for Humans-in-the-Loop: Decisions in the Presence of Erroneous Algorithmic Scores,* Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, https://doi.org/10.1145/3313831.3376638; Ben Wagner, *Liable, but not in control? Ensuring meaningful human agency in automated decision-making systems*, 11.1 Policy & Internet 104 (2019), https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.198; Ari Ezra Waldman, *Power, process, and automated decision-making*, 88 Fordham L. Rev. 613 (2019), https://ir.lawnet.fordham.edu/flr/vol88/iss2/9/?web=1&wdLOR=c3806A0EE-E5C8-0E4A-8DF2-37C30BCB1A10; Danielle Keats Citron and Frank Pasquale, *The scored society: Due process for automated predictions*, 89 Wash. L. Rev. 1 (2014), https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2/.

interested persons to sign-up for the mailing list on the Department's CPA Rulemaking webpage at coag.gov/CPA, and to check the webpage periodically for updates.