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.