Before the
Office of the Attorney General
Colorado Department of Law
Denver, CO

In the Matter of:	)	
	)	**Docket No. 4 CCR-904-3**
Colorado Privacy Act Rules	)	

Comments of the Electronic Privacy Information Center (EPIC)

Samuelson-Glushko Technology Law and Policy Clinic (TLPC) at Colorado Law

Counsel to EPIC

Xelef Botan, Tanner Kohfield, and Veronica Phifer, Student Attorneys
Blake E. Reid, Director

blake.reid@colorado.edu

via electronic submission to coag.gov

January 12, 2023

Electronic Privacy Information Center (EPIC)
1519 New Hampshire Ave, N.W.
Washington, D.C. 20036
(202) 483-1140

Alan Butler, Executive Director
Caitriona Fitzgerald, Deputy Director
John Davisson, Director of Litigation
Ben Winters, Senior Counsel
Calli Schroeder, Senior Counsel
Sara Geoghegan, Counsel
Suzanne Bernstein, Fellow

Table of Contents

Discussion

The Electronic Privacy Information Center (EPIC) is a public interest research center based in Washington, D.C. that was established in 1994 to focus public attention on emerging privacy and related human rights issues and to protect privacy, the First Amendment, and constitutional values.[1] EPIC has a long history of promoting transparency and accountability for information technology.[2] EPIC respectfully submits these comments in response to the Colorado Attorney General and the Department of Law's (collectively, the Department's) notice of proposed rulemaking (NPRM) seeking comment on proposed draft rules implementing the Colorado Privacy Act in the above-referenced docket.[3] We commend the Department for its work to establish privacy protections for Coloradans and urge the Department to revise certain provisions in its proposed rules to provide Consumers and Controllers clear guidance with respect to their rights and duties.

Below, please see our feedback to specific questions raised by the NPRM, followed by general comments on issues that are not specifically raised by the NPRM.[4] Our feedback is organized in the order of the nine sections mentioned in the NPRM. We have also included an appendix that contains suggested line edits for the following specific rules:

- Rule 2.02 DEFINED TERMS
- Rule 4.02 SUBMITTING REQUESTS TO EXERCISE PERSONAL DATA RIGHTS
- Rule 4.03 RIGHT TO OPT OUT
- Rule 4.04 RIGHT OF ACCESS
- Rule 4.05 RIGHT TO CORRECTION
- Rule 4.06 RIGHT TO DELETION
- Rule 4.07 RIGHT TO DATA PORTABILITY
- Rule 4.08 AUTHENTICATION

---

[1] EPIC, About EPIC (2022), https://epic.org/about/.

[2] *See, e.g.*, Comments of EPIC et al. to Cal. Priv. Protection Agency (June 8, 2022), https://epic.org/wp-content/uploads/2022/06/GlobalOptOut-Coalition-Letter.pdf; Comments of EPIC and Coalition to Cal. Priv. Protection Agency (Nov. 8, 2021) https://epic.org/documents/comments-of-epic-and-three-organizations-on-regulations-under-the-california-privacy-rights-act-of-2020/; Comments of EPIC to Cal. Office of the Att'y Gen. (Feb. 25, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC to Cal. Office of the Att'y Gen. (Dec. 6, 2019), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf; *see also* Comments of EPIC (Mar. 25, 2022), https://epic.org/epic-recommends-cfpb-strengthen-buy-now-pay-later-bnpl-market-inquiry-on-customer-acquisition-and-data-practices/.

[3] *Colorado Privacy Act Rules*, Notice of Proposed Rulemaking, 4 CCR 904-3 (NPRM) (Oct. 10, 2023), https://www.sos.state.co.us/CCR/DisplayHearingDetails.do?trackingNumber=2022-00603 [hereinafter NPRM].

[4] NPRM at 2.

- Rule 4.09 RESPONDING TO CONSUMER REQUESTS
- Rule 5.07 SYSTEM FOR RECOGNIZING UNIVERSAL OPT-OUT MECHANISM
- Rule 5.08 OBLIGATIONS ON CONTROLLERS
- Rule 5.09 CONSENT AFTER UNIVERSAL OPT-OUT
- Rule 6.04 CHANGES TO A PRIVACY NOTICE
- Rule 6.05 LOYALTY PROGRAMS
- Rule 6.06 PURPOSE SPECIFICATION
- Rule 6.07 DATA MINIMIZATION
- Rule 7.04 REQUESTS FOR CONSENT
- Rule 8.02 SCOPE
- Rule 8.03 STAKEHOLDER INVOLVEMENT
- Rule 8.05 TIMING
- Rule 8.06 ATTORNEY GENERAL REQUESTS
- Rule 9.06 DATA PROTECTION ASSESSMENTS FOR PROFILING

These comments and proposed edits were initially prepared in significant part based on the draft rules released on Oct. 10, 2022.[5] Based on the Department's unexpected release of a second version of draft rules with extensive revisions on Dec. 21, 2022, we have prefaced the portions of our comments that respond to the first version of the draft rules with **[v1]** and supplemented where possible with additional reactions to the most significant and substantive revisions in the second version of the draft rules, prefaced with **[v2]**. However, the large extent of the revisions and their unexpected release has prevented us from reflecting every change in the second version of the draft rules here, including in the Appendix. We ask that the Department construe these comments and proposed edits consistent with the substantive points articulated below.

Given the significant breadth, depth, and complexity of the rules, we also urge the Department to announce future revisions to the draft rules in advance, accompanied by a deadline before which comments must be received to have impact on an announced revision. Doing so would reflect typical agency comment cycles and administrative law principles and would help ensure that all commenters have reasonable notice of substantive changes and reasonable opportunities to respond in earnest to the complex substance of this rulemaking.

I. Definitions

A. Question 1—Biometric Data

[v1] The NPRM states:

> *Biometric Data.* The CPA does not define Biometric Data. The Department based the proposed definition of "biometric data" on

[5] 4 CCR-904-3, http://coag.gov/app/uploads/2022/10/CPA_Final-Draft-Rules-9.29.22.pdf [hereinafter CPA].

corresponding laws in the United States. Does this definition sufficiently capture and protect biometric information?

[v1] The current definition of Biometric Data is underinclusive and inadvisably relies on whether a Biometric Identifier is "used or intended to be used . . . for identification purposes."[6] A Controller's collection, processing, and retention of Biometric Identifiers presents heightened privacy risks to the Consumer even if the Controller never uses the data for identification purposes. For example, the risk that a malicious third party or unauthorized employee will access and misuse the Consumer's data remains the same in either case. Accordingly, such data should qualify as Biometric Data (and thus as Sensitive Data) regardless of its planned or actual use by the Controller. For the same reason, the exclusion of "any data generated from a digital or physical photograph or an audio or video recording" "[u]nless such data is used for identification purposes" from the definition of Biometric Data should be revised to "data generated from a digital or physical photograph or an audio or video recording that cannot be used to uniquely identify an individual."

[v2] We support the definition of "Biometric Identifiers" as reflected in the revised draft rules.

Consistent with the above, we propose a revised definition of "Biometric Data" as follows:

> "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, **or** (b) an audio or voice recording. **Such data also excludes** ~~*or (c)*~~ any data generated from a digital or physical photograph or an audio or video recording **that cannot be used to uniquely identify an individual.**

B. Question 2—Widely Available Information

[v1] The NPRM states:

> *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

[6] CPA Rule 2.02.

the prerulemaking period. Are there any other examples that can be provided to further refine this proposed definition?

[v1] We support the definition of "Information that a Controller has a reasonable basis to believe the Consumer has made available to the general public" (referred to for simplicity's sake as "Widely Available Information") set out in the rules, subject to three key revisions. First, the phrase "the type of information known to be available to the general public" is inconsistent with the text of C.R.S. § 6-1-1303(17)(b). With the exception of information drawn from government records, § 6-1-1303(17)(b) only excludes (otherwise personal) data from the protections of the CPA if the Controller has "reasonable basis" to believe that the Consumer "made [that information] available to the general public." But the fact that a particular type of Personal Data (e.g., a Consumer's home address) may routinely be "available to the general public" does not by itself provide a reasonable basis to conclude that *the Consumer* was responsible for such disclosure. We urge that this phrase be struck from the definition.

Second, the phrase "including but not limited to" should be changed to "which may include but is not limited to." This allows for the possibility that Personal Data fitting one of the listed categories may not satisfy the plain text of C.R.S. § 6-1-1303(17)(b) in a particular case. For example, a highly offensive disclosure of a private citizen's medical condition by a news publication would appear to satisfy the first category, but it would not support a reasonable belief that the Consumer made or intended that disclosure.

Finally, to emphasize that C.R.S. § 6-1-1303(17)(b) and the implementing definition are not intended to limit protected speech or journalistic activities, we recommend including the proviso "that nothing in this definition shall be construed to limit or diminish rights guaranteed by the First Amendment of the United States Constitution or Section 10 of the Constitution of the State of Colorado."

[v2] The proposed revision to the second category of Widely Available Information is inconsistent with the text of § 6-1-1303(17)(b) and should be reverted. The CPA excludes from its coverage information which "*the* Consumer" (i.e., the Consumer to which the information pertains) "has lawfully made available to the general public." Changing this to "***a*** consumer" in the second category would mean that Personal Data published online automatically loses CPA protection regardless of which Consumer discloses it. This would create an enormous loophole for web scrapers and data brokers, and it cannot be squared with the emphasis of § 6-1-1303(17)(b) on the apparent actions of "*the* Consumer."

Consistent with the above, we propose a revised Widely Available Information definition as follows:

> "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*~~**the** Consumer has

intentionally made available to the general public~~,~~ or information that ~~a~~**the** Consumer has made available under federal or state law, ~~*including but not limited to*~~ **which may include but is not limited to**:

1. Personal Data found in a telephone book, a television or radio program, or a national or local news publication;
2. Personal Data that has been intentionally made available by **the**~~a~~ 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**;**

Except that nothing in this definition shall be construed to limit or diminish rights guaranteed by the First Amendment of the United States Constitution or Section 10 of the Constitution of the State of Colorado.

C. Question 3—Publicly Available Information

[v1] The NPRM states:

> *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?

[v1] We support the list of data types excluded from Publicly Available Information as originally drafted, subject to our proposed amendment below.

[v2] With respect to the revised draft rules, we oppose the deletion of the phrase "Inferences made exclusively from multiple independent sources of publicly available information" from the Publicly Available Information exclusion list. Inferences drawn from publicly available information may reveal highly sensitive details about a Consumer that warrant the CPA's protection. For example, repeated visual observations of a Consumer entering and exiting the street entrance of a particular health clinic may reveal that person's health condition or reproductive health choices.

Instead, we urge the Department to reincorporate a narrower version of this exclusion: "Inferences made exclusively from multiple independent sources of publicly available information 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." This proposed revision would ensure continued protection for highly revealing inferences drawn from publicly available information; aligns with the existing definition of "Sensitive Data" under the CPA; and addresses any concerns that the scope of "Personal Data" covered by the CPA might otherwise infringe on protected speech.

Consistent with the above, we propose a revised definition of "Publicly Available Information" as follows:

> 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. Biometric Data;
> **3. Inferences made exclusively from multiple independent sources of publicly available information 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.**
> **4**. Genetic Information;
> **5**. Publicly Available Information that has been inextricably combined with non-publicly available Personal Data; or
> **6**. Nonconsensual Intimate Images known to the Controller.

II. Consumer Personal Data Rights

[v1] The Department of Law (Department) should empower Consumers[7] to make decisions implicating their personal data by implementing strong personal data rights. As drafted, the proposed rules leave too much discretion to data Controllers regarding which Consumer data requests to honor.[8] The rules should clearly spell out Personal Data Rights, avoiding ambiguity that could allow Controllers to violate Consumer rights based on different interpretations or vague language of the rules. As an overarching goal, the Department must be precise with the language of the rules to create a framework that closes potential loopholes and areas open to misuse and abuse.

In addition, Controller duties should be clearly specified regarding required responses to Consumers exercising Personal Data Rights. For example, the Right of Access should be supported by standards for the format and language to be used in documents provided in response to Consumer requests (e.g., standards that meet the needs of people with disabilities and ensure that documents are provided in commonly used formats so Consumers can easily access and use the content contained in them). Unless there is genuine risk that a request is fraudulent,

---

[7] C.R.S.§1-6-1-1303(6).

[8] C.R.S.§1-6-1-1303(7).

Controllers should not be able to dismiss or deny valid Consumer requests. Controllers must present a legitimate justification for denials of Consumer requests and relay the justification to the Consumer in a timely manner along with a list of necessary steps to remedy deficiencies in the requests, where applicable. Following the example of the CCPA,[9] the Department should take a layered approach to authentication to further safeguard sensitive personal data. We make the following specific suggestions to improve the proposed rules.

A. Question 1—Right to Opt Out

[v1] The NPRM states:

> 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." 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?

Consumers must be able to opt out of personal data collection via an easy and readily accessible mechanism. Controllers with direct Consumer relationships may be able to easily establish a "conspicuous and readily accessible location," particularly if our proposed language suggestions below are adopted. Controllers without a direct Consumer relationship with Consumers can still generally comply with the "conspicuous and readily accessible location" requirement by providing an "Opt-Out" mechanism (e.g. button, link, or header) on their main homepage, so long as it is clearly visible and the homepage is fully compliant with the specifications required in the proposed rules.

However, a location on a Controller's website is not conspicuous and readily accessible if a Consumer has no way to know that the Controller is processing that Consumer's personal data. This makes it all the more necessary that Consumers are notified that their personal data is being collected when they first visit a webpage. The conspicuous button/link, which can be in a different font/size/style, could serve as an additional reminder to Consumers.

In addition, the language used in the privacy notice and additional opt-out mechanism must be accessible and easily understood. To further that goal, we recommend adding language to proposed Rule 4.03(B)(2) to confirm that a Controller must:

---

[9] California Privacy Protection Agency, Modified Text of Proposed Regulations at 63, https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf.

> Pursuant §§ 6-1-1306(1) and 6-1-1308(1)(a)(III), provide a clear and conspicuous method for Consumers to exercise the right to opt out of the Processing of Personal Data for the Opt-Out Purposes, either directly or through a link, **in language that is clear, understandable, and free of legal or technical jargon that an average consumer might have difficulty comprehending and** in a clear, conspicuous, and readily accessible location outside **and in addition to** the privacy notice.

Furthermore, the Department should keep accessibility concerns front and center when deciding on the rules, especially as they relate to the language and formatting. Protecting personal data rights must not exclude or disadvantage persons with disabilities.

The updated version of the language in Rule 4.03(B) has removed the requirement that the opt-out location must be "[a]vailable to the Consumer at or before the time the Personal Data is Processed for the Opt-Out Purposes." However, we suggest that the following language be added, mandating that the opt-out mechanism be "Available to the Consumer at any time after they opt-in." (If a consumer opts-out at the beginning, there is no need to go over the steps enumerated in Rule 4.03, as personal data will not be collected.) The final rule would act such that Rule 4.03(B)(3)(c), as revised, would read:

> (c) The clear, conspicuous, and readily accessible location must be 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 must be available to the Consumer at any time after they opt-in.**

The Department should require Controllers to wait 24 hours before they start collecting Consumer's personal data in order to prevent mistaken opt-ins and give Consumers the opportunity to change their minds.

In situations where Consumers decide to opt out of personal data processing, Controllers must promptly notify their Processors and instruct them to honor Consumers' requests as quickly as possible. We recommend adding the following sections to Rule 4.03:

> **E. Processors who acquire or buy personal information from Controllers are required to stop processing the personal information as soon as feasibly possible, no later than seven (7) days from the receipt of notice of Consumer opt-out by a Controller.**
> **F. Controllers selling the personal data to Processors must notify those parties as soon as feasibly possible, but no later than one to five (1-5) days after receiving the opt-out notice from the Consumer.**

B. Question 2—Right of Access

[v1] The NPRM states:

> 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?

[v1] Wherever possible, a Controller should respond to a Consumer request via the method used by the Consumer (e.g., through email or a Controller's own webpage or application platform). However, responsive documents, especially those containing Sensitive Data, must be disclosed with care and caution by Controllers, lest that data be accessed by unauthorized and unintended parties.

Controllers providing requested documents must be required to make them accessible for people with disabilities. We suggest adding the below subsection to Rule 4.04(B)(1), which would mandate that the response Controllers provide to Consumers be accessible for persons with disabilities:

> **a. In the case of consumers with disabilities, the Controller provided response must be reasonably accessible. The business 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, or comparable successor standards adopted by the Consortium.**

Responsive documents must be provided in appropriate and commonly used electronic formats to ensure full exercise of Consumer data rights, allowing for ease of access and ability to understand the content. Formats with limited accessibility or that confuse or obfuscate content for Consumers would be inappropriate and would frustrate the purpose of the CPA. Accordingly, the Department should change Rule 4.04(B)(3) as fellows to best enable Consumers to make informed decisions of whether to exercise deletion, correction, or opt-out rights:

> Avoid incomprehensible internal codes and include explanations **in an appropriate commonly used electronic format, depending on the nature of the data,** that would allow the average Consumer to make an informed decision of whether to exercise deletion, correction, or opt-out rights.

The Department should also add a subsection to Rule 4.04(B)(3) to further clarify how the documents requested by Consumers should be provided. The relevant subsection would read:

a. The Personal Data provided in a request must be in a format that is downloadable by the Consumer, and machine-readable upon request to enable exercise of the right to data portability.

Controllers, in response to Consumer requests, should also provide categories of personal data collected and what is done with that data. As such, we feel inclusion of the following section under Rule 4.04(B) would strengthen the rules and give more clarity and power to Consumers on whether to exercise their data rights:

4. Be provided in a way that includes the following information:
a. The purpose for which the Personal Data was collected or sold;
b. Categories of personal information collected about the Consumer;
c. Specific pieces of personal information a business has collected about the Consumer;
d. Categories of sources from which the personal information is collected; and
e. Categories of personal information that the business sold or disclosed about the Consumer.

[v2] We appreciate the specific details added to Rule 4.04(A)(1) in the revised proposed rules noting that profiling decisions, inferences, and derivative data concerning Consumers are also covered under Personal Data. Explicitly classifying Controller created information as covered Personal Data will strengthen Consumer rights. Requiring Controllers to provide Personal Data in response to Consumer requests to "[a]void incomprehensible internal codes and include explanations" (as in revised Rule 4.04(B)(3)) will facilitate Consumers' exercise of Personal Data Rights. The changes also align with our overall recommendation that the language used by Controllers to communicate or provide documents to Consumers should be free of technical or legal jargon and easy to understand by a layperson.

C. Question 3—Right to Correction

[v1] The NPRM states:

> 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?

[v2] A Consumer can easily practice the right to correction through account settings on a Controller's webpage. So long as the process afforded to Consumers to exercise this right is easy to use and quick to implement, the language deployed in the proposed rules is effective.

However, the Department should restructure Rules 4.05(D-H) to better capture the steps that Controllers must take before they can deny Consumers' correction requests in cases where there is a disagreement as to the accuracy of Personal Data in question. If and only if a Controller exhausts all the steps enumerated in Sections D-H should a Controller be able to deny such a request. Otherwise, the proposed rules stand to give too much power to Controllers to decide unilaterally what they will accept as adequate documentation from Consumers. We propose the following restructure as the most practical way of effectuating the provision's goal of deterring Controllers from abusing the purpose of the provision, as well as the power given them by it.

> **D.** A Controller may require the Consumer to provide documentation if necessary to determine whether the Personal Data, or the Consumer's requested correction to the Personal Data, is accurate.
>
> **1.** When requesting documentation, the Controller must provide the Consumer with a meaningful understanding of why the documentation is necessary.
>
> **2.** Any documentation provided by the Consumer in connection with the Consumer's right to correction shall only be Processed by the Controller in considering the accuracy of the Consumer's Personal Data.
>
> **3.** The Controller shall implement and maintain reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, in Processing any documentation relating to the Consumer's correction request.
>
> **4.** If the Controller did not receive the Personal Data directly from the Consumer and has no documentation to support the accuracy of the Personal Data, the Consumer's assertion of inaccuracy shall be sufficient to establish that the Personal Data is inaccurate.
>
> **5.** A Controller, **after having exhausted the steps above** may decide not to act upon a Consumer's correction request if the Controller determines that the contested Personal Data is more likely than not accurate ~~*based on the totality of the circumstances.*~~ . If a Controller denies a Consumer's correction request based on the Controller's determination that the contested Personal Data is more likely than not accurate ~~*based on the totality of the circumstances*~~ , the Controller must describe in documentation required by 4 C.C.R. 904-3, Rule 6.11(A), the Consumer's requested correction to the

> Personal Data, any documentation requested from and provided by the Consumer in support of the correction request, and the reason for the Controller's determination that the Consumer's documentation was not sufficient to support the Consumer's position.

Changing the language and structure as we suggest, which includes the more granular edits noted in the Appendix, Rule 4.05, would better resolve the points of disagreement between Controllers and Consumers and lighten the burden placed on Consumers to convince the Controllers of the accuracy of the information they provide. The Department should strike a balance between reducing burdens on Consumers and preventing fraud to best serve the purpose of the CPA. In the absence of such a balance, the rules risk either giving too much discretion to Controllers, who might abuse that discretion, or forcing Controllers to take what Consumers claim as true, which might create bigger problems in cases where those claims are not true, cannot be substantiated, or are made for fraudulent purposes. Our suggested edits strive to strike that balance.

D. Question 4—Authentication

[v1] The NPRM states:

> 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?

[v1] While it is impossible to foresee every potential data security issue that might arise in the future, the rules must consider as many as possible and aim to prevent or mitigate them. To do so, there should be different levels of authentication for different kinds of data based on its importance, sensitivity, and level of risk.

The proposed authentication requirements do not currently meet the necessary standard to prevent identity theft or fraudulent and abusive activities. Controllers should be able to deny Consumer Data Rights requests only when there is risk of fraud or the data in question is sensitive and could lead to damaging consequences for Consumers if obtained by improper parties. Adding the following variegated subsections, modeled on the CCPA,[10] under Rule

[10] California Privacy Protection Agency, Modified Text of Proposed Regulations at 63, https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf.

4.08(A) would create a layered approach that would prevent abusive behavior without creating an overly burdensome process for Consumers.

> **B. If the Consumer has a password-protected account with the Controller, the Controller may authenticate the Consumer's identity through its existing authentication methods. The Controller may require the Consumer to re-authenticate their identity before exercising their rights to opt-out, correction, data portability, or deletion.**
>
> **1. In case of suspected fraudulent or abusive activity on or from the password-protected account, the Controller may pause the Consumer's request for a period of up to fifteen (15) days and require re-authentication.**
>
> **C. If the Consumer does not have or cannot access a password-protected account with the Controller, the Controller may require additional personal data from the Consumer to compare with the data already possessed by the Controller to authenticate and honor the request.**
>
> **a. The Controller may ask for up to two additional data points from the Consumer if the Consumer's exercise of their Data Right requires disclosure of non-Sensitive Data,**
>
> **b. The Controller may ask for up to three additional data points from the Consumer if the Consumer's exercise of their Data Right requires disclosure of Sensitive Data.**

When authenticating Authorized Agents, additional steps are necessary to create a secure and easy process. Authorized Agents and their authority to act on behalf of Consumers must be more clearly spelled out and the boundaries more specifically delineated to prevent abusive behavior, ensure authentic authority, and allow proper and easy exercise of that authority. It is with these concerns in mind that we recommend adopting the below additions to the rules. Authorized Agents must be required to provide proof of Customer authorization to Controllers. However, that process should not be unduly burdensome. An electronically signed authorization letter by Consumer, upon verification by Controllers, should serve as proper authentication of the Consumer's allocation of authority. For ease of reading and logical flow, we would add the below section to Rule 4.08(A):

> **D. If the request to exercise a Consumer Personal Data Right is submitted by an Authorized Agent on behalf of the Consumer, the Controller shall require the Authorized Agent to provide the Consumer's written proof of authorization before complying with the request.**
>
> **1. An Authorized Agent may provide the Consumer's authorization form directly to the Controller.**

2. An electronically signed authorization form shall be deemed sufficient.

E. Alternatively, a Consumer may provide the authentication necessary by either:

1. Logging into the Consumer's password-protected account registered with the Controller to confirm that the Authorized Agent's request is properly authorized, or

2. Verifying the authorization in another manner the Controller sets up without requiring collection of more additional Personal Data than strictly necessary.

In cases where Controllers are unable to authenticate the Consumer submitting a Data Rights request after exhausting all commercially reasonable efforts to do so, Controllers should deny such requests. Allowing exercise of Data Rights without proper authentication can easily lead to significant Consumer injury. However, denial of such requests must be clearly relayed along with information on how to remedy the deficiency in the Data Rights request or authentication. We suggest the following edits to proposed Rule 4.08(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**, in a timely manner,** inform the Consumer that their identity could not be authenticated**, provide information on how to remedy any deficiencies with the request,** and may request additional Personal Data if ~~*reasonably*~~ necessary to Authenticate the Consumer.

E. Question 5—Appeal Process

[v1] The NPRM states:

> 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?

[v2] Our proposed edits to improve the appeals process are in the Appendix, Rule 4.09. However, the rules should be as unambiguous as possible to avoid enabling Controllers to make unilateral or unsubstantiated decisions regarding exercise of Consumer Data Rights. The rules should avoid terminology such as "reasonably," "reasonably necessary," and "good faith" that gives Controllers too much discretion and raises the risk of abuse.

Additional rules would be helpful to streamline the appeals process and close potential loopholes open to abusive or capricious decision-making on the part of Controllers. The following subsection would strengthen that process if added as Rule 4.09(B)(3):

> **3. If the request appears to be fraudulent or abusive, the Controller shall notify the Consumer, through the method ordinarily used to communicate with the Consumer, of the request made on their behalf and require them to go through the authentication procedures established in Rule 4.08(A)(1)–(3) before executing any such data rights requests.**

This addition would clearly establish the responsibilities of Controllers and make abusive or fraudulent behavior much harder. The appeals process also would benefit from interpretive guidance and/or descriptions of best practices. Illustrative examples would be especially helpful.

Moreover, Controllers should be required to provide an explanation when they deny Data Rights requests. The following edit to Rule 4.09(B)(2), which otherwise is open to Controller interpretation and requires no justification for denial, would close that loophole:

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

F. General Comments on Issues Not Specifically Raised by the NPRM

There were no specific questions concerning the below proposed rules in the NPRM. However, our suggested edits below will ensure better protection of Consumers as well as facilitate the exercise of Personal Data Rights guaranteed by the CPA.

[v2] Rule 4.02 (Submitting Requests). The word "reasonably" in Rule 4.02(D) should be struck because it creates an area open to discretion of Controllers. Controllers should be permitted to request more Personal Data only where strictly necessary. In its edited form, the relevant section would read:

> 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.

While many changes to this section in v2 of the CPA were welcome, we are not sure why Rule 4.03(B)(5) prohibiting Controllers from using Dark Patterns, as defined by C.R.S. § 6-1-1303(9) and prohibited by 4 CCR 904- 3, Rule 7.09, was removed. Use of Dark Patterns by Controllers is a significant problem that curtails meaningful exercise of Data Rights. The Department should include the deleted subsection.

[v2] Rule 4.06 (Right to Deletion). The proposed rules do not specify when Controllers must delete Personal Data upon Consumer request, leaving this right open to abuse through allowing Controllers to continue to process data without necessary consent or authorization and directly against the wishes of the Consumer. A time limit on effectuating Consumer deletion

requests would better serve the goals of the CPA. We recommend adding the following subsection to Rule 4.06(A) requiring Controllers to comply with Consumers' deletion requests within 15 days:

> **4. Effectuating the request within fifteen (15) days.**

Furthermore, Controllers should be required to provide explanation for decisions to deny Consumers' deletion requests. Otherwise, the rules would allow Controllers to retain data that they are required to delete under the CPA on vague or unstated grounds. We suggest adding the following provision to Rule 4.06:

> **F. In case of a Controller denying a Consumer's deletion request in whole or in part, the Controller must provide the Consumer with a detailed explanation of the denial basis and delete all Personal Data that is not exempted under C.R.S. § 6-1-1304.**

The sole major revision to Rule 4.06 in the revised proposed rules is the addition of a new subsection under Rule 4.06(A), which in relevant part states that Controllers must ensure their Processors are also compliant vis-à-vis Consumer deletion requests. We fully support this new addition. With our above suggestions, the rest of our suggestions can be viewed in Appendix, Rule 4.06. We believe these suggestions will strengthen the Right to Deletion, empowering Consumers and removing undue Controller discretion to capriciously deny Consumer requests.

[v2] Rule 4.07 (Right to Data Portability). To better effectuate the Data Portability right—especially when significant quantities of personal and/or complex data are implicated—and to better align the right with the Right to Access, we suggest adding the following to Rule 4.07(A)'s language:

> 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**, downloadable, structured, and machine-readable** 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.

To further facilitate the exercise of Personal Data Rights, Consumers must be able to transfer their data from one Controller to another without undue burden. To help ease that process, we suggest adding the following section to Rule 4.07:

> **C. In exercising his or her right to data portability, the Consumer shall have the right to have their Personal Data transmitted directly from one Controller to another, where technically feasible.**

Adopting the above suggestion in the rules would prove especially relevant and helpful in the future, where Artificial Intelligence and other automated processes become more common.

While Controllers should not have to disclose their trade secrets when complying with Data Rights requests exercised by Consumers, trade secrets should also not be become an excuse to deny meaningful exercise of Data Rights. The revised language of Rule 4.07 strikes an appropriate balance between Consumer rights and protection of trade secrets. We believe that our edits for this rule, in addition to the new language of the revised proposed rules, will properly enable Consumers to exercise their right to Data Portability.

G. New Questions Posed in the Second Version of the Draft Regulations[11]

[v2] The revised proposed rules ask:

> We received specific feedback both in support of and against the use of IP addresses to Authenticate the location of Consumers opting out of the Sale of Personal Data or use of Personal Data for Targeted Advertising using a Universal Opt-Out Mechanism. Some commenters stressed that the use of IP addresses would be a frictionless method that is used often and should be used in this context, while others expressed concerns about consumers' ability to use an IP address that does not accurately reflect their location. What are the pros and cons of using IP addresses to Authenticate the location of Consumers opting out of the sale of Personal Data or use of Personal Data for Targeted Advertising using a Universal Opt-Out Mechanism? What are other ways for Consumers to Authenticate their location in that context?

We discuss the Universal Opt-Out Mechanism in the following section.

III. Universal Opt-Out Mechanism

[v1] We are concerned with potential issues in Rules 5.05-5.09 concerning Controllers' obligation to honor universal opt-out requests in a timely manner. Specifically, the rules should require Controllers to recognize Consumers both online and offline. The rules also should delegate specific standards to Controllers, ensuring that they are aware that they may only collect Consumers' information when cross-referencing that information to its database to guarantee that they are implementing the universal opt-out mechanism appropriately. To align with the California Consumer Privacy Act, the Department should create or mandate the use of icons and a brief statement describing the icon to ensure Consumers are notified that their universal opt-out mechanisms are honored to assist those varying in languages and cultures, and to circumvent any

[11] CPA, Version 2 of Proposed Draft Regulations at 4, https://coag.gov/app/uploads/2022/12/CPA_Version-2-Proposed-Draft-Regulations-12.21.2022.pdf [hereinafter Version 2 of Proposed Draft Regulations].

issues for people with disabilities. The public list of required signals should be updated every three months. Finally, the rules should only allow for Consumers' authentication via an Internet Protocol (IP)-to-location service or self-certification. This will limit needless data collection under the auspices of authentication.

A. Question 1—Offline Recognition

[v1] The NPRM asks:

> 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?12

[v1 & v2] Once a Controller collects an individual's identifier that matches an online account or profile, the Controller should then be required to comply with the Consumer's request for the use of a universal opt-out mechanism. Once a business or company is voluntarily provided with a Consumer's email or phone number, a Controller's online database should be used to cross-reference to an existing or counter-profile to ensure that the Controller properly honors the universal opt-out. In effect, cross-referencing the profiles will ensure proper implementation of the mechanism.

However, the proposed rules may allow a Controller to collect more information to implement the universal opt-out mechanism than is necessary. The Controller should only collect a Consumer's personal information when the Consumer offers that information. The Department should amend Rule 5.05(C) to state:

> **A Controller shall not collect a Consumer's personal data for the sole purpose of implementing the universal opt-out mechanism. Rather, the Controller should only collect a Consumer's personal information when the Consumer offers that information. When an identifier is collected offline that the Controller knows or should know is linked to an existing or counter-profile that has asserted the universal opt-out mechanism, the Controller is responsible for recognizing the opt-out mechanism. These identifiers may include a phone number or an email address.**

B. Question 2—Universal Opt-Out Mechanism List

[v1] The NPRM asks:

---

[12] NPRM at 3.

> 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?[13]

[v2] The second proposed rules ask:

> We received at least one comment regarding the process that will be followed for determining which mechanisms will be recognized by the "System for Recognizing Universal Opt-Out Mechanisms" in draft rule 5.07. The comment suggested that we provide opportunities for stakeholder participation in the process. We welcome other suggestions regarding this process.
>
> - Should the process for determining which mechanisms will be recognized be fully prescribed in this rulemaking, or can it be developed later?
> - What should the process for determining which mechanisms entail?[14]

[v1 & v2] We agree with several other commenters[15] that a public list of acceptable universal opt-out mechanisms will help lessen the compliance burden on Controllers by reducing any potential information gap. Rule 5.07 should also allow for feedback from stakeholders to help ensure interoperability, such as with other states, and to avoid potential security concerns. The Department should also provide periodic updates to the list; more specifically, Rule 5.07(A) should state:

> The initial list shall be released no later than January 1, 2024, and shall be updated **in three-month increments. Controllers should be allowed to provide recommendations for acceptable universal opt-out mechanisms through a notice-and-comment procedure. Controllers should provide suggestions to the Department.**

C. Question 3—Universal Opt-Out Mechanism Standards

The NPRM asks:

---

[13] *Id.* at 2-3.

[14] Version 2 of Proposed Draft Regulations at 4.

[15] Colorado Office of the Attorney General, *Colorado Privacy Act Stakeholder Meeting Nov. 10, 2022*, YouTube (Nov. 15, 2022), https://www.youtube.com/watch?v=-0IvsN5ald0.

> 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?[16]

Put simply, the rules should reinforce Consumers' autonomy when their information is requested and ensure that no more data than necessary is collected to implement the universal opt-out mechanism.

[v2] Rather than moving (C)'s previously third standard to additional considerations under (D), we suggest that this point should remain as a standard. Rule 5.07(C) should thus state:

> **C. To be recognized, a Universal Opt-Out Mechanism must at a minimum meet the following standards:**
>
> **1. Comply with all of the technical and other specifications of this section; Rule 5; and**
>
> **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.**
>
> **3. Not create Consumer or Controller confusion about the similarities and differences between Universal Opt-Out Mechanisms on the public list**
>
> **4. The mechanism shall only collect information when the Consumer chooses to provide that information. If the Consumer uses the universal opt-out mechanism, the Consumer's offered information should only be used to cross-reference within a Controller's database so that the Controller can properly identify a Consumer's profile or counter-profile.**

D. Question 4—Notice

[v1] The NPRM asks:

> 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?[17]

---

[16] NPRM at 3.

[17] *Id.*

[v1 & v2] We agree that Controllers should provide notice to Consumers so that Consumers understand that a universal opt-out mechanism is honored, and it must do so in a conspicuous manner. Icons have historically been used to allow Consumers to understand that certain processes are in place, such as tracking or third-party data sharing.[18] When icons are paired with a short statement describing the icons, they are useful in transcending cultural and language barriers.[19] Controllers should not be permitted to use pop-ups and banners at the bottom of the screen so as to avoid Consumer fatigue. However, the mechanism should still be put in an expected place so as to circumvent interference with a Consumer's online experience.

There is precedent in the California's Office of the Attorney General's implementation of the California Consumer's Privacy Act (CCPA), which helped create an opt-out icon in the form of a blue check mark.[20] Similarly, Rule 5.08(E) should require Controllers to notify Consumers when they are honoring the mechanism by displaying a symbol, such as a green lock. The CPA rules also can go one step further, pairing the symbol with a disappearing concise statement indicating what the symbol means, such as "Opt-Out Preference Signal Honored." In the event that the Controller may not be able to honor the universal opt-out mechanism, it should affirmatively state, "Opt-Out Signal Not Honored" to ensure Consumers are notified when the mechanism has not been effective. The icon should also be placed in the upper right-hand corner to ensure it is in an expected place. Specifically, Rule 5.08(E) should read:

> A Controller **must** display in a conspicuous manner if it has Processed the Consumer's opt-out preference signal. **The Controller shall also avoid overly burdensome signals, such as pop-ups or banners. The Controller may not use signals that are intrusive or disruptive. The Controller shall ensure the mechanism be placed in the upper right-hand corner so that it does not interfere with consumers' online experiences.**
>
> **1. The Controller must display on its website a green lock symbol, paired with a concise statement indicating what the symbol means--"Opt-Out Preference Signal Honored"--in the upper right-hand corner** when a browser, device, or Consumer utilizing a Universal Opt-Out Mechanism visits the website.
>
> **2. If the Controller cannot recognize the universal opt-out mechanism, it has an affirmative duty to notify the Consumer.**

---

[18] Hanan Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorri Faith Cranor, Joel R. Reidenberg, Norman Sadeh, Florian Schaub, *Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts*, CHI Conference on Human Factors in Computing Systems, https://dl.acm.org/doi/pdf/10.1145/3411764.3445387.

[19] *Id.*

[20] CA Office of the Attorney General, *CCPA Opt-Out Icon*, https://oag.ca.gov/privacy/ccpa/icons-download (last visited Dec. 21, 2021).

E. Question 5—Timing

[v2] With the updated version of the proposed rules, we agree that providing the list on January 1, 2024 and ensuring compliance occurs on July 1, 2024 is appropriate. However, the public list should be updated in three-month increments, rather than stating it should be "updated periodically." By opting for a less subjective phrase, Controllers will be given proper notice of any potential updates to the public list. The Department should move this objective standard with obligations for Controllers to update their mechanism.

Rule 5.07(A) should read as follows:

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

Rule 5.07(E) should state:

> E. The Colorado Department of Law will allow Controllers **three (3)** months to recognize Universal Opt-Out Mechanisms added to the public list.

F. Question 7—Authentication

[v1] The NPRM asks:

> 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?[21]

[v1 & v2] Rule 5.08 provides that the Controller must be able to accurately authenticate the Consumer's residency for proper enforcement of the universal opt-out mechanism. The Controller may be entitled to authenticate the source of an opt-out signal via an IP-to-location service or self-certification. The rules should not obligate Consumers to create an account or log-in to verify their residencies, nor require any other affirmative step beyond self-certification for purposes of proper enforcement of the universal opt-out mechanism. Specifically, the Rule 5.08(D) should be edited to:

---

[21] *Id.*

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 Authenticate themself as a condition of recognizing the Consumer's use of a Universal Opt-Out Mechanism. Rather, the Controller may authenticate the source of an opt-out signal via an IP-to-location service. A Controller may not subject a Consumer to undertake any authentication actions that are unnecessary or unnecessarily burdensome.

IV. Controller Obligations

A. General Comments

EPIC commends the Department for providing clear and comprehensive duties for Controllers, including detailed requirements for privacy notices and purpose specification for the use of Personal Data. It is also encouraging that the draft grounds purpose specification in a data minimization framework by distinguishing requirements for secondary use.

EPIC is pleased to see the following changes in the Controller Obligation section from Version 1 to Version 2: (1) the explicit addition of third parties to the non-exhaustive list of material changes to a privacy notice in Rule 6.04(A); and (2) the conversion of the period to a semi-colon at the end of Rule 6.10(B)(1) to clarify that the list of requirements to process Sensitive Data is cumulative.

The Department should maintain the requirement from Version 1 in Rule 6.04(B) that Controllers must provide notice before a material or substantive change to a privacy policy goes into effect. Examples of substantive or material changes include critical aspects of a privacy policy, like the Controller's identity and sharing personal data with third parties. This requirement is key to achieve effective, sustained notice to Consumers.

Second, the Department should strengthen and sharpen language instructing Controllers how to appropriately narrow their purpose specification. Rule 6.06(C) should be modified as follows:

> 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*~~ **not identify**~~*ing*~~ one broad purpose to justify numerous Processing activities that are only remotely related.
> 2. Controllers should ~~*avoid*~~ **not specify**~~*ing*~~ one broad purpose to cover potential future Processing activities that are only remotely related.

Finally, the Department should maintain the requirement in Rule 6.07(B)(2) from version 1 for Controllers to obtain yearly consent to process Biometric Identifiers or any Personal Data generated from photographs or auto or visual recordings if stored for more than one year.

Biometric information is particularly sensitive. Yearly consent is an appropriate safeguard for the risks associated with continued storage, and an effective way to ensure ongoing awareness of, and access to, Consumer Personal Data rights.

B. Question 1 – Interoperability

[v2] The NPRM asks:

> How else can the Draft Rules be made interoperable with California's privacy notice requirements, while still considering the CPA's purpose specification, secondary use requirements, and ensuring that a Consumer has a meaningful understanding of the way their Personal Data will be used when they interact with a Controller?

The Draft Rules will likely be fairly interoperable with California's privacy notice requirements, notably enabled by Rule 6.02(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." Considering the CPA's purpose specification and requirements for secondary use, the California privacy notice similarly requires Controllers to inform Consumers about the intended purposes for each category of personal information collected.[22]

V. Bona Fide Loyalty Programs

The proposed versions of Rules 2.02 and 6.05 may enable Controllers to use Bona Fide Loyalty Programs to undermine the rights that the CPA confers to Consumers and the duties that the CPA places on Controllers.

Consumers do not waive rights or duties under the CPA when participating in a Bona Fide Loyalty Program. Therefore, the Department should examine whether Rule 6.05 aligns with the CPA's narrow language concerning Bona Fide Loyalty Programs. Additionally, the definition of Bona Fide Loyalty Program in Rule 2.02 should be enhanced with language that clarifies what is not considered a Bona Fide Loyalty Program. The Department should also examine Rule 6.05 while considering the guiding principle that a Bona Fide Loyalty Program's value comes from customer retention and not the sale of a Consumer's Personal or Sensitive Data. Rule 6.05 should be adjusted in line with this principle to ensure that Bona Fide Loyalty Programs do not become data monetization schemes and Consumers do not have to choose between receiving a Bona Fide Loyalty Program Benefit and waiving their rights under the CPA.

---

[22] Cal. Civ. Code §1798.130(a)(5).

A. Aligning Rule 6.05 with the Narrow Language of the Colorado Privacy Act

The Department should review whether Rule 6.05 aligns with the CPA's narrow language concerning Bona Fide Loyalty Programs. According to the CPA, a Controller may offer a "different price, rate, level, quality, or selection of goods and services to a Consumer, including offering goods or services for no fee, if the offer is related to a Consumer's voluntary participating in a Bona Fide Loyalty, Rewards, Premium Features, Discount, or Club Card Program."[23] Therefore, while Consumers participating in a Bona Fide Loyalty Program can be offered different prices or services, they still retain all rights enumerated in C.R.S. § 1-6-1-1306, and Controllers still owe them all duties enumerated in C.R.S. § 1-6-1-1308. To hold otherwise would be adding words to the statute.[24]

Currently, Rule 6.05 does not reflect that the CPA only permits Controllers to offer different prices and services to Consumers enrolled in a Bona Fide Loyalty Program. For example, Rule 6.05(B) and (D) force Consumers to choose between exercising their data rights and maintaining their Bona Fide Loyalty Program Benefit. Additionally, Rule 6.05(E) implies that Controllers can collect and sell a Consumer's Sensitive Data through a Bona Fide Loyalty Program. This rule may contradict various duties in the CPA, such as the duty of data minimization and duty to avoid secondary use. The broad array of duties in the CPA should be understood to curb Controllers' ability to collect Sensitive Data through a Bona Fide Loyalty Program if that data is not truly necessary for the program.

Consumers participating in a Bona Fide Loyalty Program under Rule 6.05 may be forced to waive various rights and duties found in the CPA. We explore these examples and others in greater detail below. However, beyond our proposed changes, the Department should review Rule 6.05 in its entirety to ensure that this rule does not include any implications that duties and rights from the CPA are waived through a Consumer's participation in a Bona Fide Loyalty Program.

B. Question One—Definition

[v1 & v2] The NPRM states:

> 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

---

[23] C.R.S.§1-6-1-1308(1)(d).

[24] *People v. Diaz*, 347 P.3d 621, 625 (Colo. 2015) ("But, in interpreting a statute, we must accept the General Assembly's choice of language and not add or imply words that simply are not there.").

> additional factors that should be considered in determining whether a loyalty program is bona fide? [25]

Version 2 of Proposed Draft Rules states:

> Commenters have expressed that the definition of "Bona Fide Loyalty Program" in the CPA rules should be made narrower and more precise. How can "Bona Fide Loyalty Programs" be defined more narrowly? Make makes a loyalty program "Bona Fide"?[26]

The proposed definition of "Bona Fide Loyalty Program" does not provide sufficient clarity as to when the CPA's loyalty program provisions apply. The definition should include clear examples describing the bounds of what is considered to be a Bona Fide Loyalty Program. Additional factors that should be considered in determining whether a loyalty program is "bona fide" are:

- Whether the program's sole purpose is to provide a Bona Fide Loyalty Program Benefit;
- Whether the program involves a direct relationship between the Consumer and the Controller; and
- Whether the Bona Fide Loyalty Program Benefit is only available to program participants.

Bona Fide Loyalty Programs should consist of simple exchanges where Consumers voluntarily participate to receive a Bona Fide Loyalty Program Benefit and Controllers are permitted to collect and process only the data that is necessary to provide the Consumer with the Bona Fide Loyalty Program Benefit. The current definition in Rule 2.02 allows programs that go beyond this simple exchange to be considered Bona Fide Loyalty Programs. For example, a program could be established for the genuine purpose of providing discounts, rewards, or other actual value to Consumers that voluntarily participate in that program, thereby fitting the current definition in Rule 2.02. However, that program could have an additional purpose, such as profiting from the sale of Personal Data of program participants to third parties. This action may be permissible under the draft Rules because Rule 2.02 does not forbid Bona Fide Loyalty Programs from having dual purposes.

This is unacceptable. Bona Fide Loyalty Programs should not be complex schemes that profit from Consumer's data while providing Consumers with only a marginal benefit. Instead, they should exist solely to provide customers with a benefit. The current draft definition of Bona Fide Loyalty Programs enables Controllers to construct programs that monetize Consumer's Personal Data and Sensitive Data through targeted advertising and sales to third parties.

---

[25] NPRM at 5.

[26] Version 2 of Proposed Draft Regulations at 4.

Controllers could profit extensively from these purported Bona Fide Loyalty Programs so long as they also provide Consumers with a Bona Fide Loyalty Program Benefit.

The Department should prevent Controllers from warping Bona Fide Loyalty Programs beyond the narrow language of the CPA by narrowing the definition in Rule 2.02 to exclude programs with any other purpose besides providing a Bona Fide Loyalty Program Benefit to Consumers. This can be achieved by adding examples of what is not a Bona Fide Loyalty Program to the definition of Bona Fide Loyalty Programs in Rule 2.02:

> **A Bona Fide Loyalty Program is not:**
>
> **1. A third-party service that offers superior prices, rates, levels, quality, or selection of goods or services from a variety of Controllers to a Consumer participating in the third-party service.**
>
> **2. A program that collects Consumers' data for any other purpose besides using that data to provide a Bona Fide Loyalty Program Benefit to Consumers.**
>
> **3. A program that sells Personal Data or Sensitive Data to Third Parties.**
>
> **4. A program that Processes Personal or Sensitive Data for Targeted Advertising.**
>
> **5. A program that collects any Personal or Sensitive Data of a Consumer beyond what is necessary to prove a Bona Fide Loyalty Program Benefit.**

Another factor to consider when determining if a loyalty program is bona fide is whether the program involves a direct relationship between the Consumer and the Controller. Currently, there are third-party services that automatically give Consumers coupons and discounts from various Controllers when a Consumer is shopping online.[27] Third-party services raise a question under the current definition of Bona Fide Loyalty Program: is a Consumer "voluntarily participating" in a Controller's Bona Fide Loyalty Program if they voluntarily participate in a third-party service that enrolls that Consumer in a Bona Fide Loyalty Program?

The answer should be no. To voluntarily participate in a Bona Fide Loyalty Program, a Consumer must sign up for the program through the Controller directly. If this was not the case, a Consumer who enrolled in a third-party service may might themselves also enrolled in hundreds, or even thousands, of Bona Fide Loyalty Programs. If a Consumer joins a Controller's Bona Fide Loyalty Program through automatic enrollment by a third party, then they did not

---

[27] PayPal Honey, https://www.joinhoney.com/ (last visited Dec. 21, 2022) (An example of this service is PayPay Honey. PayPal Honey's website states "Still looking for codes on your own? We'll search for them so you don't have to. If we find working codes, we'll automatically apply the best one to your cart." The website also boasts that it automatically applies coupons when Consumers shop at over 30,000 online stores.).

voluntarily choose to participate in that program. To avoid having Consumers that use third-party services unwittingly become Bona Fide Loyalty Program participants under these rules, we propose the following additional language to Rule 2.02:

> **A Consumer that is automatically enrolled in a Controller's Bona Fide Loyalty Program by an entity other than the Controller has not voluntarily participated in that Program. A Bona Fide Loyalty Program is not a third-party service that offers superior prices, rates, levels, quality, or selection of goods or services from a variety of Controllers to a Consumer participating in the third-party service.**

A third factor to use when determining if a loyalty program is bona fide is whether the program offers a benefit exclusively to program participants. Bona Fide Loyalty Programs should be defined as an exchange. If Consumers join a Bona Fide Loyalty Program and give the Controller a benefit, such as frequently shopping with the Controller, the Controller should be responsible for giving a Consumer a benefit that rewards them for their participation in the program. Therefore, any discount or reward that is available to Consumers not participating in a Bona Fide Loyalty Program should not be considered a Bona Fide Loyalty Program Benefit under these rules. To clarify this point in Rule 2.02, we suggest the following language be added to the definition of Bona Fide Loyalty Program Benefit:

> "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 **exclusively** through a Bona Fide Loyalty Program.

Finally, Version 2 of Proposed Draft Rules asks if a distinction should be drawn in the Rule 2.02 definition of Bona Fide Loyalty Program between programs offering rewards, premium features, discounts, or club card programs.[28] The Department should not draw such a distinction. It would create confusion for both Controllers and Consumers if the CPA and the Draft Rules applied differently based on how a Bona Fide Loyalty Program was designed. Each loyalty program's design will be slightly different and may contain components of a club card and a discount, making classifying that program difficult. The Department can avoid this confusion by viewing Bona Fide Loyalty Programs as simple exchanges where a Consumer gets a Bona Fide Loyalty Program Benefit. The exact manner in which the Consumer receives this benefit, whether it be through a discount or using a club card, is irrelevant. Question Two—Value, Benefits, and the Sale of Personal Data.

[v1 & v2] The NPRM states:

---

[28] Version 2 of Proposed Draft Regulations at 4.

> 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? [29]

Additionally, Version 2 of the Proposed Draft Rules states:

> How often do Controllers sell the Personal Data through a loyalty program? For what purpose? What are the benefits of loyalty programs to Controllers? What portion of the benefits to Controllers stems from the sale of Personal Data collected through the loyalty program versus through Consumer loyalty?[30]

[v2] Controllers may respond to these questions by claiming that selling the Personal or Sensitive Data of Consumers to Third Parties is a significant source of value and a significant benefit provided to them by their loyalty programs. While Bona Fide Loyalty Programs might include the collection of Personal Data from Consumers, the actual value and benefit of a Bona Fide Loyalty Program to Controllers should not come from monetizing the Personal or Sensitive Data collected through the program. This means that Controllers should not use Bona Fide Loyalty Programs as mechanisms to profit through the collection and sale of Consumers' Personal Data to third parties.

Loyalty programs have produced value to Controllers in ways outside of data monetization, like customer retention. From their earliest inception, loyalty programs have been a way for businesses to reward customers for their frequent patronage.[31] Loyalty programs have been around for centuries, and they only became associated with data collection in the past few decades.[32] Companies can receive value from loyalty programs through customer retention, increased spending from loyal customers, and positive word of mouth advertising.[33] For their

---

[29] NPRM at 5.

[30] Version 2 of Proposed Draft Regulations at 5.

[31] Nada Elnahla & Leighann Neilson, *The history of retail loyalty programs in North America*, Proceedings of the 20th Biennial Conference on Historical Analysis and Research in Marketing, Vol. 20, 92-95 (2021), https://www.researchgate.net/publication/354010438_The_history_of_retail_loyalty_programs_in_North_America_Extended_abstract.

[32] *Id.* at 94.

[33] *See* Julien Boudet, Jess Huang & Ryter von Difloe, *Coping with the big switch: How paid loyalty programs can help bring consumers back to your brand*, McKinsey & Co. (Dec. 21, 2022), https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/coping-with-the-big-switch-how-paid-loyalty-programs-can-help-bring-consumers-back-to-your-brand; Jess Huang, Phyllis Rothschild, & Jamie Wilkie, *Why Customer Experience Is Key for Loyalty Programs*, MIT Sloan Management Review (Dec. 21, 2022), https://sloanreview.mit.edu/article/why-customer-experience-is-key-for-loyalty-programs/.

part, Consumers do not think that their participation in a Bona Fide Loyalty Program should result in their data being collected and sold by Controllers. One study showed that 91% of US adults do not think it is a fair tradeoff for companies to give them a discount in exchange for secretly collecting information.[34]

Controllers can, and historically have, derived value and benefited from loyalty programs in ways that do not involve profiting off of the sale of a Consumer's data. For their part, Consumers would prefer to not unknowingly exchange their data for the value offered by a loyalty program However, when Controllers are allowed to sell Personal and Sensitive Data collected through loyalty programs to third parties, it results in incentives for Controllers to collect more Sensitive and Personal Data than necessary to operate a loyalty program. To prevent this outcome, honor Consumer wishes, and stay in line with historical precedent, the Department should evaluate Rule 6.05 with the understanding that the value and benefit of loyalty programs to Controllers is customer loyalty and retention, not data monetization.

The sale of Personal Data is not necessary for a loyalty program. A Bona Fide Loyalty Program should be a simple, direct exchange where a Controllers gives the Consumer a benefit and only collects the Personal Data necessary for the benefit. The sole purpose of a Bona Fide Loyalty Program should be to provide a Consumer with a Bona Fide Loyalty Program Benefit, and the value of a Bona Fide Loyalty Program to Controllers should be increased customer retention. Selling Personal Data is not necessary for Controllers to effectuate a loyalty program's purpose or receive a loyalty program's value. If the sale of Personal Data is necessary to maintain a program, either because that is the primary way Controllers derive value from that program or that is the Controller's purpose for operating the program, that program should not be considered a Bona Fide Loyalty Program. Therefore, the definition of Bona Fide Loyalty Programs in Rule 2.02 should include the following language:

> **A Bona Fide Loyalty Program is not:**
>
> **3. A program that sells Personal Data or Sensitive Data to Third Parties.**

Finally, the questions asked in Version 2 of the Proposed Draft Rules imply that the Department will consider whether and how much Controllers currently benefit from the sale of Personal Data through their loyalty programs in determining if Bona Fide Loyalty Programs under the CPA should include the sale of Personal Data.

---

[34] Michael Hennessy, Jospeh Turow, & Nora Draper, *The Tradeoff Fallacy - How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation*, Annenberg School for Communication 2, 12 (2021), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1554&context=asc_papers.

The Department should define Bona Fide Loyalty Programs to exclude programs that sell Personal Data, regardless of whether Controllers currently benefit from this practice. The core concern of the Department should be drafting rules that benefit Consumers, not drafting rules that conform to current Controller practices.

Furthermore, if Controllers are currently substantially benefitting from the sale of Personal Data through loyalty programs, that is all the more reason to exclude the sale of Personal Data in Bona Fide Loyalty Programs. If the practice is widespread, it shows that Controllers view loyalty programs not as simple exchanges, but as opportunities to further monetize Consumers Personal Data. Therefore, the Department should adopt our proposed changes to the Rule 6.05 to curb the use of Bona Fide Loyalty Programs as methods to collect and profit from a Consumer's Personal and Sensitive Data, undermining core protections enshrined in other parts of the CPA.

C. Question Three—Disclosures

[v1 & v2] The NPRM States: Are there different or additional disclosures that should be made to Consumers concerning Bona Fide Loyalty Programs?[35] As a threshold matter, the Department should delete Rule 6.05 (E)(b)-(d) in its entirety. Additionally, the Department should add two additional disclosures that will ensure great transparency to Consumers in the areas of Personal and Sensitive Data.

Rule 6.05(E)(1)(b) implies that Controllers can sell Consumer's Personal and Sensitive Data to third parties. Rule 6.05(E)(1)(c)-(d) also implies that Controllers can sell Personal Data to third parties and process Personal Data for Targeted Advertising. These subsections imply that using Bona Fide Loyalty Programs as methods of monetizing a Consumer's Personal and Sensitive Data through the sale of that data to Third Parties is acceptable as long as this behavior is disclosed to the Consumer.

As we explained in our response to Question 2,[36] a Bona Fide Loyalty Program's sole purpose should be to provide Consumers with a Bona Fide Loyalty Benefit. Any value that a Controller receives from a Bona Fide Loyalty Program should be through increased customer retention and loyalty. In effect, a program that creates value to the Controller by selling Consumer data to third parties or processing that data for targeted advertising is not a Bona Fide Loyalty Program; it is a data monetization scheme. Therefore, Bona Fide Loyalty Programs should not involve the sale or processing for targeted advertising of Personal and Sensitive Data, regardless of whether these activities are disclosed to Consumers. Thus, the Department should delete Rule 6.05(E)(1)(b)-(d) so customers are not forced to choose between a Bona Fide Loyalty Program Benefit and the sale of their Sensitive and Personal Data.

---

[35] NPRM at 5.

[36] *See* discussion *supra*, V.B.

In addition to our proposed deletion, we have two proposed additions to Rule 6.05(E). First, we propose an additional disclosure that is meant to prevent Controllers from erroneously claiming that a Consumer exercising their right to delete Personal Data impacts their participation in a Bona Fide Loyalty Program. The new language in Rule 6.05(E) would read:

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

There may be times when a Consumer's decision to exercise their right to delete Personal Data impacts their participation in a Bona Fide Loyalty Program because the deleted Personal Data is necessary to effectuate the Bona Fide Loyalty Program Benefit. However, Rule 6.05 gives Controllers the exclusive authority to determine when Personal Data is necessary for a Bona Fide Loyalty Program. We are concerned that Controllers may misuse this authority by claiming Personal Data is necessary for a Bona Fide Loyalty Program when the Bona Fide Loyalty Program could be run effectively without the Personal Data collected.

To prevent misuse, if a Controller claims that a Consumer's deletion of Personal Data makes it impossible to provide that Consumer with a Bona Fide Loyalty Benefit, the Controller must also disclose an explanation to that Consumer. This disclosure will create greater transparency to Consumers. Additionally, it will incentivize Controllers to make accurate decisions regarding whether Personal Data is actually necessary for a Bona Fide Loyalty Program because Controllers know that they will have to explain any decision they make to Consumers.

Second, we propose the following additional disclosure to prevent Controllers from collecting Sensitive Data that is unnecessary for a Bona Fide Loyalty Program. Sensitive Data should rarely, if ever, be required for a Bona Loyalty Program Benefit. However, if a Controller claims that their Bona Fide Loyalty Program requires Sensitive Data, then they should be required to disclose to Consumers why this is the case. The new language in Rule 6.05(E) would read:

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

There is precedent in the CCPA for requiring Controllers to disclose why they made certain decisions about a Consumer's data, which is what our proposed additional disclosures in Rule 6.05 (E) seek to do. The CCPA allows businesses to offer financial incentives to Consumers for the collection and sale of personal information and offer a different price if that price difference

is reasonably related to the value provided to the business by the Consumer's data.[37] Subsequently, the California Attorney General issued a rule that requires companies offering financial incentives for Consumer's personal information to disclose to Consumers an explanation of how the financial incentive is reasonably related to the value of a Consumer's data.[38] The Department should follow this example from the CCPA and implement our additional disclosures so that Controllers are required to explain certain decisions they make concerning Bona Fide Loyalty Programs.

D. Question Four—Guidance

[v1 & v2] The NPRM states: Are there aspects of the loyalty program statutory provisions or draft rules that can benefit from more guidance?[39] Version 2 of the Proposed Draft Rules also states:

> Under the CPA, why and when should Controllers be able to prevent a Consumer from obtaining the benefits of a bona fide loyalty program despite that Consumer's decision to opt out of the sale of Personal Data, or Processing of Personal Data for Targeted Advertising or Profiling in furtherance of decisions that produce legal or similarly significant effects concerning a Consumer?[40]

As we have frequently emphasized in this section[41], Consumers participating in a Bona Fide Loyalty Program should retain all rights enumerated to them in C.R.S.§1-6-1-1306. Additionally, the value of Bona Fide Loyalty Programs should be seen as customer loyalty and not data monetization. Therefore, a Consumer that exercises a data right, including their right to opt out of the sale or processing or profiling of Personal Data, should not lose their ability to receive a Bona Fide Loyalty Program Benefit. Only the Consumer's decision to exercise the right to delete Personal Data should ever implicate Bona Fide Loyalty Programs. To help Rule 6.05 better reflect this reality, we propose an additional section be added to this rule. We also propose changes to the current Rule 6.05(B), (D), and (F).

New Section of Rule 6.05. First, we propose adding a new section to the beginning of Rule 6.05 that would expressly affirm that participation in a Bona Fide Loyalty Program does not impact the rights and duties from the CPA. The new Rule 6.05(A) would state:

---

[37] Cal. Civ. Code § 1798.125(b)(1).

[38] Cal. Code Regs § 999.307(5).

[39] NPRM at 5.

[40] Version 2 of Proposed Draft Regulations at 5.

[41] *See* discussion *supra*, V.A–C.

A Consumer who voluntary participates in a Bona Fide Loyalty Program has not waived any rights enumerated in C.R.S.§1-6-1-1306. A Controller is not relieved of any duties enumerated in C.R.S.§1- 6-1-1308 if a Consumer voluntarily participates in Controller's Bona Fide Loyalty Program. A Consumer's participation in a Bona Fide Loyalty Program only allows a Controller to offer a different price, rate, level, quality, or selection of goods and services to that Consumer. A Controller's duty of data minimization extends to Bona Fide Loyalty Programs. Therefore, a Controller's collection of Personal Data through a Bona Fide Loyalty Program shall be adequate, relevant, and limited to what is reasonably necessary to provide a Consumer with a Bona Loyalty Program Benefit.

This proposed addition to Rule 6.05 explicitly mentions a Controller's duty of data minimization. This duty is particularly important because it prevents Controllers from turning Bona Fide Loyalty Programs into large-scale data collection regimes that collect more data than necessary to offer a Bona Fide Loyalty Program Benefit. As we previously addressed,[42] aspects of Rule 6.05 could be interpreted as endorsing the idea that Consumers waive their data rights through participation in a Bona Fide Loyalty Program. Therefore, this proposed addition is needed to ensure that Controllers do not erroneously interpret the CPA and Rule 6.05 to mean that Consumers waive their data rights through participation in a Bona Fide Loyalty Program.

Rule 6.05(C). Rule 6.05(C) allows Controllers to discontinue a Bona Fide Loyalty Program Benefit if a Consumer refuses to consent to the Processing of Sensitive Data necessary for a Bona Fide Loyalty Program Benefit. Sensitive Data should rarely, if ever, be necessary for a Bona Fide Loyalty Program Benefit. C.R.S.§1-6-1-1303(24) defines Sensitive Data as "Personal Data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status." Controllers, through the duty of minimization in C.R.S.§1- 6-1-1308(3), are limited to collecting Personal Data that is adequate, relevant, or reasonably necessary to the purpose for which the data is being processed. As we earlier argued,[43] the sole purpose of a Bona Fide Loyalty Program is to provide Consumers with a Bona Fide Loyalty Program Benefit, so all data collected must be reasonably necessary for this purpose. Therefore, it is unlikely that the categories of Sensitive Data described in C.R.S. 6-1-1303(24) will ever be necessary to provide a Bona Fide Loyalty Program Benefit.

If Rule 6.05(C) is left unchanged, Controllers could use this rule to force Consumers to choose between consenting to the collection of their Sensitive Data and receiving a Bona Fide Loyalty Program Benefit. But, as explained above, a Consumer should almost never have to give

---

[42] *See* discussion *supra*, V.A) and V.D).

[43] *See* discussion *supra*, V.B.

up Sensitive Data to receive a Bona Fide Loyalty Program Benefit. Therefore, if Controllers claim Sensitive Data is necessary to provide a Bona Fide Loyalty Program, they should have the burden of explaining to Consumers why this is the case. For that reason, we offer the following language to be added to the beginning 6.05(C):

> **It is presumed that personalized Bona Fide Loyalty Program Benefits will not require the Processing of Sensitive Data. Controllers have the burden of proving to Consumers why their Sensitive Data is necessary for a Bona Fide Loyalty Program Benefit.**

Rule 6.05(D). Rule 6.05 (D) states that if a Consumer exercises a Data Right that impacts their membership in a Bona Fide Loyalty, a Controller can then discontinue that Consumer's Bona Fide Loyalty Program Benefit. This provision is overinclusive because the only Data Right that should implicate Bona Fide Loyalty Programs is the right to delete Personal Data. A Consumer exercising other rights in C.R.S.§1-6-1-1306, including their rights of access, right to correction, and right to data portability would have no impact on Controllers collecting the Personal Data necessary to effectuate a Bona Fide Loyalty Program Benefit.

Additionally, a Consumer exercising their right to opt out of the sale of Personal Data, Processing of Personal Data for Targeted Advertising or Processing of Personal Data for Profiling in furtherance of decisions that produce legal or similarly significant effects concerning a Consumer should note lose their Bona Fide Loyalty Program Benefit. As we explained in our answer to Questions One and Two,[44] Controllers should only collect the Personal Data necessary to effectuate a Bona Fide Loyalty Program Benefit. Controllers should not collect Personal Data as part of a Bona Fide Loyalty Program in order to process that data for targeted advertising, sale to third parties, or making decisions about that Consumer.

We are concerned that if Rule 6.05(D) is left in its current form, Controllers could use this provision to force their Consumers to choose between receiving their Bona Fide Loyalty Program Benefit and exercising their statutory rights from the Colorado Privacy Act. This contradicts the language of the CPA, which makes no mention of Consumers waiving their Personal Data rights by joining a Bona Fide Loyalty Program. To prevent Controllers from potentially misusing Rule 6.05(D), we propose narrowing the language of Rule 6.05(D) to state:

> If a Consumer's decision to exercise ~~*a Data Right*~~ **their right to delete Personal Data** impacts the Consumer's membership in a Bona Fide Loyalty Program, the Controller shall notify the Consumer of the impact of the Consumer's decision in conformance with 4 CCR 904-3, Rule 3.02 and at least twenty-four (24) hours before discontinuing the Consumer's

[44] *See* discussion *supra*, Parts V.C–D.

Bona Fide Loyalty Program Benefit or membership, and must provide a reference or link to the information required by subparagraph E., below.

We also recommend the following new language to Rule 6.05(B) so that it is consistent with our proposed changes to Rule 6.05(D):

> **A Controller shall not discontinue a Consumer's Bona Fide Loyalty Program Benefit because of a Consumer's decision to exercise a Personal Data right except** 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.

Rule 6.05(F) Finally, we propose that additional examples be added to Rule 6.05(F). These examples will illustrate various points we have made throughout our responses to the questions from the NPRM, including: programs that are operated for purposes other than providing a Consumer with a Bona Fide Loyalty Program Benefit are not Bona Fide Loyalty Programs, a Consumer's decision to not consent to the collection of Sensitive Data should not normally impact their ability to receive a Bona Fide Loyalty, and Consumers who exercise their right to opt out from the CPA should not lose their Bona Fide Loyalty Benefit. The new examples we propose be added to Rule 6.05(F) are:

> **2. A Consumer joins a program offered by a pharmacy that collects a Consumers' Personal Data to provide that Consumer with a discount. This program also sells the Consumer's Personal Data to Third Parties. This program is not a Bona Fide Loyalty Program because it does not have the genuine and sole purpose of providing discounts, rewards, or other actual value to Consumers that voluntarily participate in that program.**
> **3. A Consumer joins a pharmacy's Bona Fide Loyalty Program. Later, that Consumer does not consent to the processing of their Sensitive Data. The Sensitive Data is not necessary for the Consumer's Bona Fide Loyalty Program Benefit. Under these circumstances, the Controller cannot discontinue the Consumer's Bona Fide Loyalty Program Benefit.**
> **4. A Consumer joins a pharmacy's Bona Fide Loyalty Program. Later, that Consumer exercises their right to opt out of the sale of Personal Data. Under these circumstances, the Controller cannot discontinue the Consumer's Bona Fide Loyalty Program Benefit. This is because Controllers can only discontinue a Consumer's Bona Fide Loyalty**

Program if that Consumer exercise their right to delete Personal Data and the Personal Data deleted is necessary to provide the Bona Fide Loyalty Program Benefit

E. General Comments on Additional Issues Raised by the Revised Draft Rules

Rule 6.05, as well as the definitions of Bona Fide Loyalty Program and Bona Fide Loyalty Program Benefit from Rule 2.02, are unchanged in the Department's Version 2 of Proposed Draft Rules. Therefore, the changes we have suggested for Rule 2.02 and Rule 6.05 apply to both versions of the proposed rules. The above sections answer the questions about Bona Fide Loyalty Programs raised by the Department in its initial NPRM. Additionally, we have addressed the questions about Bona Fide Loyalty Programs raised in the Department's Version 2 of Proposed Draft Rules in sections B, C, and E above.

VI. Consent

EPIC previously submitted comments regarding consent under the CPA. We reiterate the concerns and support from those comments and write here to offer new suggestions for the second version of the proposed draft rules.

A. Question 1—Consent Elements

The NPRM asks:

> 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?[45]

In general, EPIC supports the strong consent requirements for valid consent provided by the CPA. We suggest including an additional example about the implementation of "Refreshing Consent" to clarify what are permissible and impermissible means of obtaining consent after 12 months of inactivity.

The rules should also clarify what a "similar number of steps" in a consent scheme looks like in the context of refusing or revoking consent, *see* Rule 7.07(A). A narrow interpretation of "similar" in this context is appropriate because the process for refusing or revoking consent should be as easy as the process for obtaining consent.

---

[45] NPRM at 5.

EPIC supports the new language in Section 7.05 which prohibits consent fatigue-inducing schemes, as explained in our previous comments.

The revised draft rules helpfully clarify what constitutes "substantial effect of subverting or impairing user autonomy, decision making or choice" in a consent interface design or choice architecture,[46] which will ensure improved compliance.

B. Question 2—Examples

The NPRM asks:

> 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?

Regarding Rule 7.03(D)(1)(a), EPIC encourages the Department to add an example that clarifies what types of processing purposes would be similar enough to require only a single consent option. For example, if a Controller obtains valid Consent to process a Consumer's personal information to provide customer support services, the Controller may process that information to send a communication to the Consumer to inquire about the Consumer's satisfaction with the customer support. Similarly, if a Controller obtains valid Consent to process a Consumer's personal information to fulfill the Consumer's order, the Controller may process that personal information to provide tracking updates to the Consumer. However, if a Controller obtains valid Consent to process a Consumer's personal information for order fulfillment purposes, the Controller may not process that personal information to send promotional materials to the Consumer because that purpose is unrelated to the original processing purpose.

C. Additional Recommendations

We recommend that the Department make changes to the examples following Rule 7.04 in order to clarify when personal contact information can be used to solicit Consent for secondary uses. The examples in subpart E, as drafted, are potentially confusing and overbroad. The example in subpart E.1 implies that it would be appropriate for a company to use personal contact information in a special-purpose product recall list to make a general solicitation for Consent to receive promotional advertising materials in the future. The examples should be modified to make clear that a general-purpose customer contact list could be used for this purpose of soliciting consent to secondary marketing, but not the product recall list, consistent with Rule 6.08. We propose the example be modified as follows:

---

[46] Version 2 of Proposed Draft Regulations at 31-32.

E. Example: Acme Toy Store collects customer email addresses in order to send customers information about ~~*product recalls*~~ **their orders** and maintains those email addresses in a ~~*recall*~~ **customer** email distribution list **for purposes including completing the customer's order, processing payment, and providing shipping updates**. Acme Toy Store wants to use the ~~*recall*~~ customer email distribution list to send those customers promotional materials. Acme Toy Store must obtain customer consent prior to using the ~~*recall*~~ customer email distribution list to provide promotional materials because providing promotional materials is not necessary to or compatible with providing ~~*product recall*~~ **customer order** information. Acme Toy Store emails the ~~*recall distribution*~~ **customer email** 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*~~ **customer** 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 **not** valid because the ~~*email contained all required Consent disclosures in an acceptable form.*~~ consent solicitation is itself incompatible with the primary purpose of the list, per Rule 6.08(B).

2. Example: Under the same circumstances, Acme Toy Store emails the ~~*product recall*~~ **customer information** email distribution list informing those customers that it would like to use their email addresses for the secondary purpose of providing promotional materials as contemplated in section B.2.e. of its privacy notice, explains that it cannot use the customers' email addresses for that secondary purpose without their consent, and requests the customers' Consent to process their email address for that secondary purpose. It then provides a link directly to section B.2.e. of its privacy notice which explains that Acme Toy Store 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.

VII. Data Protection Assessments

[v2] EPIC commends the Department for making the requirements and timing of data protection assessments in Part 8 both protective and straightforward for Controllers to follow. In particular, changing "describe each of" to "include" in Rule 8.04(A) is important to clarify the duty of Controllers and to ensure that the data protection assessment is not merely a box-checking exercise. The specificity of elements laid out in Rule 8.04 are clear and not overly burdensome. However, EPIC is concerned about some of the changes to the regulations released on December 21 and accordingly makes the following recommendations:

- Include a specific time period of 14 days before beginning processing to Rule 8.05(A); and
- Include a specific time period of one year to replace the less clear "periodical" updates to the data protection assessment in Rule 8.05(B).

A. Question 1 – Clarity and Purpose of Assessment Content

[v1] The NPRM states:

> 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?

Overall, the draft rules do not make the requirements overly burdensome. The Department can avoid data protection assessments becoming a mere check-the-box exercise by: requiring certain aspects of the assessment to be made public; requiring involvement of all relevant external parties in completion of the data protection assessment; adding a requirement for a signed certification of completeness and accuracy by an Executive Officer; requiring identification of certain minimum operational elements of the Processing Activity; clarifying a specific time period when updates to the data protection assessment are required; adding a specific time period requirement for completion before processing can continue or begin; and clarifying rules about interoperability with data protection assessments required by other jurisdictions. Below, EPIC will offer statutory suggestions to implement these suggestions.

To implement the requirement of including all relevant external parties in completion of the data protection assessment, EPIC recommends the following change:

> 8.03(A). A data protection assessment ~~*should*~~ **shall** involve all relevant internal actors from across the Controller's organizational structure, and

~~*where needed, relevant*~~ external parties **involved in the processing,** to identify, assess and address the data protection risks.

To implement EPIC's recommendation to clarify timing obligations for Controllers to complete a data protection assessment, the following changes should be made:

> 8.05(A). A Controller shall conduct and document a data protection assessment **14 days** 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).
> 8.05(B) A Controller shall review and update the data protection assessment ~~*periodically*~~ **once yearly** throughout the Processing activity's lifecycle…

To implement the requirement that an Executive Officer certifies the completeness and accuracy of the data protection assessment, EPIC recommends the following addition to Rule 8.06:

> **8.06(B). When submitting the data protection assessment to the Attorney General, an Executive Office of the Controller must attest to the completeness and accuracy of the document.**

To implement the clarification about using data protection assessment submissions previously used in other jurisdictions, EPIC recommends the following change:

> 9.06(H). If a Controller conducts a data protection assessment which includes an assessment of relevant Profiling for the purpose of complying with another jurisdiction's law or regulation, the **Controller may submit that assessment with a supplement that contains any additional information required by this jurisdiction.** ~~*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.*~~

B. Question 2 – Burden

[v1] The NPRM states:

> Are the DPA requirements expressed in the draft rules overly burdensome on smaller businesses? How so? How can they be made less burdensome?

No, the data protection assessment regulations do not pose requirements that are overly burdensome on small businesses. Smaller businesses are less likely to be processing extremely large amounts of data which would make compliance with the requirements a simpler exercise, and Regulation 8.02(C) explicitly recognizes the proportional burden for the amount of data

processed. In order to strengthen the privacy protections for consumers, consistent with the Department's goal, EPIC recommends the following change to Rule 8.02:

> 8.02(C) – The depth, level of detail, and scope of data protection assessments ~~*should*~~ **must** be proportionate to the size of the Controller, amount and sensitivity of Personal Data Processed, and Personal Data Processing activities subject to the assessment.

Conclusion

EPIC applauds the Department's open and robust rulemaking process to protect Consumers in accordance with the Colorado Privacy Act. We will continue to be available for discussion about our recommendations and about how the Department can best protect Coloradans under the CPA, and we look forward to participating in future stages of this process.

Appendix—Recommended Changes

Rule 2.02 DEFINED TERMS

"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, **or** (b) an audio or voice recording**. Such data also excludes** ~~*or (c)*~~ any data generated from a digital or physical photograph or an audio or video recording **that cannot be used to uniquely identify an individual.**

"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 **and sole** purpose of providing discounts, rewards, or other actual value to Consumers that voluntarily participate in that program. **A Consumer that is automatically enrolled in a Controller's Bona Fide Loyalty Program by an entity other than the Controller has not voluntarily participated in that Program.**

A Bona Fide Loyalty Program is not:

1. A third-party service that offers superior prices, rates, levels, quality, or selection of goods or services from a variety of Controllers to a Consumer participating in the third-party service.

2. A program that collects Consumers' data for any other purpose besides using that data to provide a Bona Fide Loyalty Program Benefit to the Consumer.

3. A program that sells Personal Data or Sensitive Data to Third Parties.

4. A program that Processes Personal or Sensitive Data for Targeted Advertising.

5. A program that collects any Personal or Sensitive Data of a Consumer beyond what is necessary to prove a Bona Fide Loyalty Program Benefit to that Consumer.

"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 **exclusively** through a Bona Fide Loyalty Program.

"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*~~ **the** Consumer has intentionally made available to the general public~~,~~ or information that ~~*a*~~ **the** Consumer has made available under federal or state law, ~~*including but not limited to*~~ **which may include but is not limited to**:

1. Personal Data found in a telephone book, a television or radio program, or a national or local news publication;
2. Personal Data that has been intentionally made available by **the**~~*a*~~ 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**;**

Except that nothing in this definition shall be construed to limit or diminish rights guaranteed by the First Amendment of the United States Constitution or Section 10 of the Constitution of the State of Colorado.

"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. Biometric Data;
3. **Inferences made exclusively from multiple independent sources of publicly available information 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.**
4. Genetic Information;
5. Publicly Available Information that has been inextricably combined with non-publicly available Personal Data; or
6. Nonconsensual Intimate Images known to the Controller.

[v1] Rule 4.02 SUBMITTING REQUESTS TO EXERCISE PERSONAL DATA RIGHTS

[…] 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, **and the request submission process works otherwise,** 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.

[v2] Rule 4.03 RIGHT TO OPT OUT

A. A Controller shall comply with an opt-out request **of a consumer who had originally opted in** 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 **in language that is clear, understandable, and free of legal or technical jargon that an average consumer might have difficulty comprehending** as well as in a clear, conspicuous, and readily accessible location outside **and in addition to** 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." **"Colorado Privacy Opt-Out"**

2. Pursuant §§ 6-1-1306(1) and 6-1-1308(1)(a)(III), provide a clear and conspicuous method for Consumers to exercise the right to opt out of the Processing of Personal Data for the Opt-Out Purposes, either directly or through a link, **in language that is clear, understandable, and free of legal or technical jargon that an average consumer might have difficulty comprehending and** in a clear, conspicuous, and readily accessible location outside **and in addition to** the privacy notice.

3. 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 easy-to-follow and execute instructions that are accessible to all consumers, including people with disabilities on how to opt out.

c. The clear, conspicuous, and readily accessible location must be 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 must be available to the Consumer at any time after they opt-in.**

C. Controllers should wait 24 hours before they start collecting Consumer's personal data to prevent mistaken opt-ins and give the Consumer some time to change their mind.

D. 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.

E. Processors who acquire or buy personal information from Controllers are required to stop processing the personal information as soon as feasibly possible, no later than seven (7) days from the receipt of notice of Consumer opt-out by a Controller.

F. Controllers selling the personal data to processors must notify those parties as soon as feasibly possible, but no later than one to five (1-5) days after receiving the opt-out notice from the Consumer.

[v2] 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.

a. In the case of consumers with disabilities, the Controller provided response must be reasonably accessible. The business 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, or comparable successor standards adopted by the Consortium.

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

3. Avoid incomprehensible internal codes and include explanations **in an appropriate commonly used electronic format, depending on the nature of the data,** that would allow the average Consumer to make an informed decision of whether to exercise deletion, correction, or opt-out rights.

a. The Personal Data provided in a request must be in a format that is downloadable by the Consumer, and machine-readable upon request to enable exercise of the right to data portability.

4. Be provided in a way that includes the following information:

a. The purpose for which the Personal Data personal information was collected or sold;

b. Categories of personal information collected about the Consumer;

c. Specific pieces of personal information a business has collected about the Consumer;

d. Categories of sources from which the personal information is collected; and

e. Categories of personal information that the business sold or disclosed about the Consumer.

C. A Controller shall not be required to disclose in response to an access request a Consumer's government-issued identification number**, social security number,** financial account number**s,** 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.

D. If a Consumer exercises the right to access their data in a portable format pursuant to C.R.S. § 6-1-1306(1)(e) and the Controller determines the manner of response would reveal the Controller's trade secrets, the Controller must still honor the Consumer's undiminished right of access in a format or manner which would not reveal trade secrets, such as in a nonportable format.

[v2] 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, except archive or backup systems, and implementing measures to ensure that the Personal Data remains corrected. The Controller shall also instruct alluse the technical and organizational measures or process established by its 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 **across all systems that the Consumer's Personal Data is processed.**

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

restored to an active system or is next accessed or used for a Sale, disclosure, or commercial purpose.

C. 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, time consuming, or difficult** to the Consumer;

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

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

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

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

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

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

3. The Controller shall implement and maintain reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, in Processing any documentation relating to the Consumer's correction request.

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

5. A Controller, **after having exhausted the steps above** may decide not to act upon a Consumer's correction request if the Controller determines that the contested Personal Data is more likely than not accurate ~~*based on the totality of the circumstances.*~~. If a Controller denies a Consumer's correction request based on the Controller's determination that the contested Personal Data is more likely than not accurate ~~*based on the totality of the circumstances*~~ , the Controller must describe in documentation required by 4 C.C.R. 904-3, Rule 6.11(A), the Consumer's requested correction to the Personal Data, any documentation requested from and provided by the Consumer in support of the correction request, and the reason for

the Controller's determination that the Consumer's documentation was not sufficient to support the Consumer's position.

[v2] 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);

2. Using the technical and organizational measures or process established by its Processors to delete the Consumer's Personal Data held by the Processors; ~~and~~

3. Notifying the Controller's Affiliates to delete the Consumer's Personal Data obtained from the Controller~~.~~**; and**

4. Effectuating the request within fifteen (15) days.

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 the categories 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, **and notifying all of the Controller's Processors and Affiliates to do the same.**

F. In case of a Controller denying a Consumer's deletion request in whole or in part, the Controller must provide the Consumer with a detailed explanation of the denial basis and delete all Personal Data that is not exempted under C.R.S. § 6-1-1304.

[v2] 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**, downloadable, structured, and machine-readable** 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. When complying with a request to access Personal Data in a portable format, Controllers must provide as much data as possible in a portable format without disclosing the trade secret.

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

C. In exercising his or her right to data portability, the Consumer shall have the right to have their Personal Data transmitted directly from one Controller to another, where technically feasible.

[v1] Rule 4.08 AUTHENTICATION

[…]

B. If the Consumer has a password-protected account with the Controller, the Controller may authenticate the Consumer's identity through its existing authentication methods. The Controller may require the Consumer to re-authenticate their identity before exercising their rights to opt-out, correction, data portability or deletion.

1. In case of suspected fraudulent or abusive activity on or from the password-protected account, the Controller may pause the Consumer's request for a period of up to fifteen (15) days and require re-authentication.

C. If the Consumer does not have or cannot access a password-protected account with the Controller, the Controller may require additional personal data from the Consumer to compare with the data already possessed by the Controller have to authenticate and honor the request.

1. The Controller may ask for up to two additional data points from the Consumer if the Consumer's exercising their data right requires disclosure of data that is not sensitive,

2. The Controller may ask for up to three additional data points from the Consumer if the Consumer's exercising their data right requires disclosure of Sensitive Data.

D. If the request to exercise a Consumer Personal Data Right is submitted by an Authorized Agent on behalf of the Consumer, the Controller shall require the Authorized Agent to provide the Consumer's written proof of authorization before complying with the request.

1. An Authorized Agent may provide the Consumer's authorization form directly to the Controller.

2. An electronically signed authorization form shall be deemed sufficient.

E. Alternatively, a Consumer may provide the authentication necessary by either:

1. Logging into the Consumer's password-protected account registered with the Controller to confirm that the Authorized Agent's request is properly authorized, or

2. Verifying the authorization in another manner the Controller sets up without requiring collection of more additional Personal Data than strictly necessary.

F. 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.

[…]

J. 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**, in a timely manner,** inform the Consumer that their identity could not be authenticated**, provide information on how to remedy any deficiencies with the request,** and may request additional Personal Data if ~~*reasonably*~~ necessary to Authenticate the Consumer.

[v1] 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.

a. If the request appears to be fraudulent or abusive, the Controller shall notify the Consumer, through the method ordinarily used to communicate with the Consumer, of the request made on their behalf and require them to go through the authentication procedures established in Rule 4.08(A)(1)–(2) before executing any such data rights requests.

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 **state the grounds for denial of request and** 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.

[v2] Rule 5.05 PERSONAL DATA USE LIMITATIONS

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

B. When processing a Universal Opt-Out Mechanism, a Controller may not require the collection of additional Personal Data beyond that which is strictly necessary to authenticate a Consumer is a resident of Colorado 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. **A Controller shall not collect a Consumer's personal data for the sole purpose of implementing the universal opt-out mechanism. Rather, the Controller should only collect a Consumer's personal information when the Controller offers that information. When an identifier is collected offline that the Controller knows or should know is linked to an existing or counter-profile that has asserted the universal opt-out mechanism, the Controller is responsible for recognizing the opt-out mechanism. These identifiers may include a phone number or an email address.**

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

[v2] Rule 5.07 SYSTEM FOR RECOGNIZING UNIVERSAL OPT-OUT MECHANISMS

A. The Colorado Department of Law shall maintain a public list of Universal Opt-Out Mechanisms that have been recognized to meet the standards of this subsection. The initial list shall be released no later than January 1, 2024 and shall be updated **in three-month increments. Controllers should be allowed to provide recommendations for acceptable universal opt-out mechanisms through a notice-and-comment procedure. Controllers should provide suggestions to the Department.**

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

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

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

2. 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.

4. The mechanism shall only collect information when the consumer chooses to provide that information. If the consumer uses the universal opt-out mechanism, the consumer's offered information should only be used to cross-reference within its information database a consumer's profile or counter-profile to appropriately implement the opt-out mechanism.

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.

E. The Colorado Department of Law will allow Controllers **three (3)** months to recognize Universal Opt-Out Mechanisms added to the public list.

[v2] 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 all purposes, as indicated by the mechanism, for the associated browser or device, and, if known, for the Consumer.

2. After receiving a valid opt-out request through the use of a Universal Opt-Out Mechanism, a Controller shall continue to treat the browser, device, and Consumer as having exercised opt-out rights until the browser, device, or Consumer overrides the optout, 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.

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 Authenticate themself as a condition of recognizing the Consumer's use of a Universal Opt-Out Mechanism. Rather, the Controller may authenticate the source of an opt-out signal via an IP-to-location

service. A Controller may not subject a Consumer to undertake any authentication actions that are unnecessary or unnecessarily burdensome.

E. A Controller **must** display in a conspicuous manner if it has Processed the Consumer's opt-out preference signal. **The Controller shall also avoid overly burdensome signals, such as pop-ups or banners. The Controller may not use signals that are intrusive or disruptive. The Controller shall ensure the mechanism be placed in the upper right-hand corner so that it does not interfere with consumers' online experiences.**

1. The Controller must display on its website a green lock symbol, paired with a concise statement indicating what the symbol means--"Opt-Out Preference Signal Honored"--in the upper right-hand corner when a browser, device, or Consumer utilizing a Universal Opt-Out Mechanism visits the website.

2. If the Controller cannot recognize the universal opt-out mechanism, it has an affirmative duty to notify the Consumer.

Rule 6.04 CHANGES TO A PRIVACY NOTICE

[…]

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

[v2] Rule 6.05 LOYALTY PROGRAMS

A. A Consumer who voluntary participates in a Bona Fide Loyalty Program has not waived any rights enumerated in C.R.S.§1-6-1-1306. A Controller is not relieved of any duties enumerated in C.R.S.§1- 6-1-1308 if a Consumer voluntarily participates in that Controller's Bona Fide Loyalty Program. A Consumer's participation in a Bona Fide Loyalty Program only allows a Controller to offer a different price, rate, level, quality, or selection of goods and services to that Consumer. A Controller's duty of data minimization extends to Bona Fide Loyalty Programs. Therefore, a Controller's collection of Personal Data through a Bona Fide Loyalty Program shall be adequate, relevant, and limited to what is reasonably necessary to provide a consumer with a Bona Loyalty Program Benefit.

~~*A.*~~ **B.** 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.*~~ **C. A Controller shall not discontinue a Consumer's Bona Fide Loyalty Program Benefit because of a Consumer's decision to exercise a Personal Data right except** 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.*~~ **D. It is presumed that personalized Bona Fide Loyalty Program Benefits will not require the Processing of Sensitive Data. Controllers have the burden of proving to Consumers why their Sensitive Data is necessary for a Bona Fide Loyalty Program Benefit.** 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.*~~ **E.** If a Consumer's decision to exercise ~~*a Data Right*~~ **their right to delete Personal Data** 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 3.0102 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.*~~ **F.** Loyalty Program Disclosures

1. In addition to all other disclosures required by 4 CCR 904-3, Rules 6.03 and 7.03, a Controller maintaining a Bona Fide Loyalty Program must provide the following disclosures 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. If a Controller claims that a Consumer's decision to delete Personal Data makes it impossible to provide a Bona Fide Loyalty Program Benefit, then the Controller shall provide that Consumer with an explanation of why the

deletion of Personal Data makes it impossible to provide a Bona Fide Loyalty Benefit

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

~~*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.*~~ **G.** Example**s**:

1. 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. **The Sensitive Data is necessary to provide the personalized Bona Fide Loyalty Program Benefit.** 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.

2. A Consumer joins a program offered by a pharmacy that collects a Consumers' Personal Data to provide that Consumer with a discount. This program also sells the Consumer's Personal Data to Third Parties. This program is not a Bona Fide Loyalty Program because it does not have the genuine and sole purpose of providing discounts, rewards, or other actual value to Consumers that voluntarily participate in that program.

3. A Consumer joins a pharmacy's Bona Fide Loyalty Program. Later, that Consumer does not consent to the processing of their Sensitive Data. The Sensitive Data is not necessary for the Consumer's Bona Fide Loyalty Program Benefit. Under these circumstances, the Controller cannot discontinue the Consumer's Bona Fide Loyalty Program Benefit.

4. A Consumer joins a pharmacy's Bona Fide Loyalty Program. Later, that Consumer exercises their right to opt out of the sale of Personal Data. Under these circumstances, the Controller cannot discontinue the Consumer's Bona Fide Loyalty Program Benefit. This is because Controllers can only discontinue a Consumer's Bona Fide Loyalty Program if that Consumer exercise their right to delete Personal Data and the Personal Data deleted is necessary to provide the Bona Fide Loyalty Program Benefit.

Rule 6.06 PURPOSE SPECIFICATION

[…]

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*~~ **not identify**~~*ing*~~ one broad purpose to justify numerous Processing activities that are only remotely related.

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

Rule 6.07 DATA MINIMIZATION

[…]

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 Date 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. Such assessment shall be documented according to 4 CCR 904-3, Rule 6.11. **Controllers must obtain Consent to Process Biometric identifiers or any Personal Data generated from a digital or physical photograph or an audio recording each year after the first year that it is stored.**

Rule 7.04 REQUESTS FOR CONSENT

[…]

E. Example:

1. Acme Toy Store collects customer email addresses in order to send customers information about ~~product recalls~~ **their orders** and maintains those email addresses in a ~~recall~~ **customer** email distribution list **for purposes including completing the customer's order, processing payment, and providing shipping updates**. Acme Toy Store wants to use the ~~recall~~ customer email distribution list to send those customers promotional materials. Acme Toy Store must obtain customer consent prior to using the ~~recall~~ customer email distribution list to provide promotional materials because providing promotional materials is not necessary to or compatible with providing ~~product recall~~ **customer order** information. Acme Toy Store emails the ~~recall distribution~~ **customer email** 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.

2. Under the same circumstances, Acme Toy Store emails the ~~recall~~ **customer** 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 **not** valid because the ~~email contained all required Consent disclosures in an acceptable form.~~ consent solicitation is itself incompatible with the primary purpose of the list, per Rule 6.08(B).

3. Under the same circumstances, Acme Toy Store emails the ~~product recall~~ **customer information** email distribution list informing those customers that it would like to use their email addresses for the secondary purpose of providing promotional materials as contemplated in section B.2.e. of its privacy notice, explains that it cannot use the customers' email addresses for that secondary purpose without their consent, and requests the customers' Consent to process their email address for that secondary purpose. It then provides a link directly to section B.2.e. of its privacy notice which explains that Acme Toy Store 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 8.02 – SCOPE

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

Rule 8.03 – STAKEHOLDER INVOLVEMENT

A. A data protection assessment ~~*should*~~ **shall** involve all relevant internal actors from across the Controller's organizational structure, and ~~*where*~~

~~*needed, relevant*~~ external parties **involved in the processing**, to identify, assess and address the data protection risks. […]

Rule 8.05 - TIMING

A. A Controller shall conduct and document a data protection assessment **14 days** 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 ~~*periodidcally*~~ **once yearly** throughout the Processing activity's lifecycle…

Rule 8.06 - ATTORNEY GENERAL REQUESTS

B. When submitting the data protection assessment to the Attorney General, an Executive Office of the Controller must attest to the completeness and accuracy of the document.

Rule 9.06 – DATA PROTECTION ASSESSMENTS FOR PROFILING

H. If a Controller conducts a data protection assessment which includes an assessment of relevant Profiling for the purpose of complying with another jurisdiction's law or regulation, **the Controller may submit that assessment with a supplement that contains any additional information required by this jurisdiction.** ~~*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.*~~