

COLORADO DEPARTMENT OF LAW

Consumer Protection Section

Colorado Privacy Act Rules

4 CCR 904-3

PART 2 DEFINITIONS

Rule 2.02 DEFINED TERMS

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

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

“Biometric Identifier” is defined as set forth in C.R.S. § 6-1-1303(2.45), and means data generated by the technological processing, measurement, or analysis of an individual’s biological, physical, or behavioral characteristics, which data can be Processed for the purpose of uniquely identifying an individual. Biometric Identifier includes a fingerprint; a voiceprint; a scan or record of eye retina or iris; a facial map, facial geometry, or facial template; or other unique biological, physical, or behavioral patterns or characteristics.

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

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

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

PART 6 DUTIES OF CONTROLLERS

Rule 6.13 DUTY REGARDING MINOR DATA – KNOWLEDGE STANDARD

- A. The following factors may be considered when determining if a Controller willfully disregards that a Consumer is a Minor as contemplated in C.R.S. § 6-1-1308.5:
1. If the Controller has directly received information from a parent or Consumer indicating that the Consumer is a Minor.
 - a. Example: A Controller requires or allows Consumers to provide their date of birth at sign up and the Consumer indicates they are a Minor.
 - b. Example: A Controller requires Consumers to provide their date of birth at sign up, which can be edited once registration is completed. A Consumer uses a fake birthdate to sign up and subsequently revises their birthdate after registration to indicate that they are a Minor.
 - c. Example: A Controller receives a credible report from a parent about a Minor using the service.
 - d. Example: A Consumer provides their age in the bio section of the profile on a Consumer's service indicating that they are a Minor.
 - e. Example: A Consumer provides relevant indicia that they are a Minor, such as year of birth or grade level, in the profile or account set up of a service.
 2. If the Controller has directed the website or service to Minors, considering different factors such as subject matter, visual content, language, and use of Minor-oriented activities and incentives.
 - a. Example: A Controller creates and distributes marketing and promotional materials related to the website or service that specifically appeal to Minors.
 3. If the Controller has categorized a Consumer as a Minor for marketing, advertising, or internal business purposes.
 - a. Example: A Controller uses Consumer data (such as user-generated content or data provided by a third party) to estimate a Consumer's age, which indicates that they are a Minor, and the Controller serves ads to them based on that estimation.
- B. In addition to the factors included in this part 4 CCR 904-3, Rule 6.13, Controllers may consider statutes, administrative rules, and administrative guidance concerning age knowledge standards from other jurisdictions when evaluating the appropriateness of treating a Consumer as a Minor as contemplated in C.R.S. § 6-1-1308.5.
- C. Consistent with C.R.S. § 6-1-1304(3)(f), nothing in this part shall require a Controller or Processor to implement an age verification or age-gating system or otherwise affirmatively collect the age of consumers.

Rule 6.14 DUTY REGARDING MINOR DATA – SYSTEM DESIGN FEATURES

- A. The following factors may be considered when determining if a system design feature significantly increases, sustains, or extends a Minor's use of an online service, product, or feature and is subject to the consent requirement as contemplated in C.R.S. § 6-1-1308.5:
-

1. Whether the controller developed or deployed the system design feature in order to significantly increase, sustain, or extend a Minor's use of or engagement with an online service, product, or feature;
 2. Whether the system design feature has been shown to increase use of or engagement with an online service, product, or feature beyond what is reasonably expected of that particular type of online service, product, or feature when it is used without the system design feature;
 3. Whether the system design feature has been shown to increase the addictiveness of the online service, product or feature, or otherwise harm Minors when deployed in the specific context offered by the Controller.
- B. A system design feature will likely not be found to significantly increase, sustain, or extend a Minor's use of an online service, product, or feature:
1. If the Minor expressly and unambiguously requested specific media, the Minor subscribed to specific media by the author, creator, or poster, or the Minor has subscribed to a page or group featuring specific media, provided that the media is not recommended, selected, or prioritized for display based, in whole or in part, on other information associated with the Minor or the Minor's device;
 2. If media are recommended, selected, or prioritized only in response to a specific search inquiry by the Minor, or is exclusively next in a pre-existing sequence from the same author, creator, poster, or source;
 3. If the system design feature is one that is necessary to the core functionality of an online service, product, or feature;
 4. If the system design feature is based on information that is not persistently associated with the Minor or the Minor's device;
 5. If the system design feature does not consider the Minor's previous interactions with media generated or shared by other Consumers; or
 6. If the online service, product, or feature contains countervailing measures that could mitigate the harm or other negative effects of the system design feature, such as default time of day or time use limits.
- C. The fact that a system design feature is commonly used is not, alone, enough to demonstrate that any particular feature does not significantly increase, sustain, or extend a Minor's use of an online service, product, or feature.
- D. In addition to the factors included in this part 4 CCR 904-3, Rule 6.13, Controllers may consider statutes, administrative rules, and administrative guidance concerning system design features from other jurisdictions when evaluating the likelihood that a system design feature significantly increases, sustains, or extends a Minor's use of an online service, product, or feature as contemplated in C.R.S. § 6-1-1308.5.

PART 7 CONSENT

Rule 7.03 REQUIREMENTS FOR VALID CONSENT

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

3. If a system design feature that significantly increases, sustains, or extends a Minor's use of an online service, product, or feature is turned off by default and the Minor turns on or enables the feature, such an act will be considered an affirmative action for the purpose of valid Consent as contemplated by C.R.S. § 6-1-1308.5.A short summary of the Processing activity.