DAVIS + GILBERT

Privacy + Data Security

Colorado Privacy Act Draft Rules Issued

The Bottom Line

- The Colorado Attorney General's Office has publicly committed to try to harmonize its consumer privacy law with those in California and elsewhere. However, that lofty goal may not be reached.
- As with the current draft of the CPRA regulations, the Colorado Privacy Act Draft Rules will no doubt go through additional iterations before its full scope and compliance effects are known.
- Until then, companies should consider how to address the Draft Rule's provisions while working toward compliance with other states' privacy laws.

The Colorado Attorney General's Office released Draft Rules for the Colorado Privacy Act (CPA). Issued on September 30, 2022 the Draft Rules address how the CPA will be implemented when it takes effect on July 1, 2023. A public comment period began Oct. 10 and will close Feb. 1, when the Colorado AG's Office will hold a public hearing. Therefore, we are still months away from seeing the final CPA rules.

However, given the upcoming requirements under the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA) and new laws in Utah and Connecticut, companies subject to the CPA should begin assessing their compliance obligations well before the new law takes effect.

Companies working toward CCPA/CPRA and VCDPA compliance will find that many requirements in the CPA Draft Rules overlap in large part with California's and Virginia's laws. The CPA itself follows the VCDPA fairly closely. Nevertheless, important distinctions in handling sensitive data, consumer-facing obligations and data management will require attention as companies harmonize their privacy practices under various state laws.

Below are summaries of some notable distinctions in the CPA Draft Rules. To see the complete Draft Rules, click here.

Novel Definitions

Sensitive Data Inferences

The Draft Rules create a new category called "sensitive data inferences." By using personal information collected from a consumer, a company may infer a sensitive data category, and such inferences are treated as sensitive data. For example, a company may infer the sensitive religious belief data category based on the consumer's disclosing a dietary restriction. Generally, sensitive data inferences are treated as sensitive data collected directly from the consumer would be and, therefore, cannot be processed without first obtaining consumer consent. However, a controller may process sensitive data inferences from consumers over age 13 without obtaining consent, under certain conditions.

Biometric Data

The Draft Rules' treatment of biometric data resembles the CCPA's in many respects. However, the regulations introduce two new terms, "biometric identifiers" and "biometric data," which have similarities to the Illinois Biometric Information Privacy Act (a law that often serves as the basis for class action lawsuits). Biometric identifiers refers to data generated by the processing, measurement or analysis of an individual's biological, physical or "behavioral characteristics." Biometric data is a broader term that refers to biometric identifiers used for identification purposes.

Bona Fide Loyalty Programs

Bona fide loyalty programs are established for the "genuine purpose" of providing discounts, rewards or "other actual value" to consumers. The Draft Rules provide guidance on how consumer rights requests affect businesses' loyalty programs and the disclosures required for such programs. In a nod toward practicality, the Draft Rules do not obligate a company to provide loyalty program benefits to a consumer if that consumer's rights decisions, such as deletion or withholding consent to process sensitive information, would render the company's ability to provide program benefits impossible.

Consumer Rights and Requests

Methods

The Draft Rules' process for consumers to submit requests are similar to the CCPA's. The submission methods need not be Colorado-specific but must clearly indicate that they are available to Colorado consumers, provide all data rights available to Colorado consumers (including the right to correction, which is not available under the CCPA, but is under the CPRA), provide a clear explanation of how to exercise consumer rights and satisfy the Draft Rules' general notice requirements.

Opt-out Requests

Consumers must be provided with a method to opt out of personal data processing, including sensitive data. This option can either be provided directly or through a clear and conspicuous link in its privacy notice and in a readily accessible location outside its privacy notice. If a link to opt out is used, it must take the consumer directly to the opt-out method. Within 15 days of receiving a valid opt-out request, processing of that consumer's personal data must cease.

Authenticating Consumer Requests

Authentication requirements under the Draft Rules do not differ materially from those found in the CCPA. Companies must establish "reasonable" methods to authenticate a consumer who submits a data rights request. The reasonableness of any method depends on the specific rights exercised, the risk that improper access to personal information could cause to the consumer and the value, amount and sensitivity of the personal data associated with the request.

Universal Opt-out Mechanisms

The Draft Rules include universal opt-out mechanisms (UOOM) details for a straightforward way for consumers to exercise opt-out rights with all controllers with which they interact, rather than making individual requests with each. Controllers must offer the means for consumers to provide an affirmative, freely given and unambiguous choice to opt out of personal data processing for targeted advertising, sales or both.

The lengthy UOOM provisions that controllers must adhere to cover notice and choice, acceptable default settings, technical specifications for recognizing and honoring opt-out requests, controllers' obligations after receiving an opt-out request and consumers' choice to consent to processing after having opted out through a UOOM. The Draft Rules state that the Colorado Department of Law will maintain a public list of UOOMs that meet the standards of the CPA's final implementing rules. The list will be created by April 1, 2024.

Controllers' Obligations

The Draft Rules contain obligations for controllers that generally follow those of the CCPA and VCDPA, but several differences merit attention:

- Privacy notices must clearly indicate which data subject rights are available to Colorado residents. The CPA grants consumers the right to confirm whether a controller is processing their personal data and access to that data; to correct inaccuracies in their personal data; to delete their personal data; to obtain a copy of personal data that they have provided to the controller in a portable format and to opt out of several types of processing, including the sale of personal data and the use of personal data for targeted advertising or profiling that produces a legal or similar effect.

- Controllers must disclose the "express purposes" for which each type of personal data is collected and processed in sufficient detail to provide consumers with a "meaningful understanding of how their personal data is used and why their personal data is reasonably necessary for the processing purpose." This purpose-driven requirement differs from CCPA's focus on the categories of data collected and how they are sold or shared.
- The Draft Rules adhere to the principles of purpose specification and data minimization, where only the minimum consumer personal data may be collected for the processing purpose(s) specified at the time of collection. The determination of such purposes must be documented and personal data that allows identification of consumers should be kept only so long as necessary, adequate or relevant to the specified, express purpose(s).
- Secondary Use – the processing of personal data for a purpose that is not reasonably necessary or compatible with the purpose(s) stated at the time of collection – is permissible only when controller obtains consumer consent for such additional processing.

Consent

Controllers will have to obtain consumer consent for, among other purposes, the processing of sensitive data. Such consent must reflect a consumer's clear, affirmative choice, be freely given, be specific and informed, and reflect the consumer's unambiguous agreement with such processing – a standard that mirrors the requirements under the European Union's General Data Protection Regulation (GDPR). The Draft Rules state that consent can be withdrawn. The Draft Rules also introduce the requirement of "refreshing consent," where a company must "refresh" consent at unstated intervals, except in connection with sensitive data, which must be refreshed annually. Further, the Draft Rules agree with the CPRA draft regulations in that both prohibit controllers from using "dark patterns" that improperly coerce or manipulate a consumer into providing consent.

Profiling

The Draft Rules create three tiers of profiling that distinguish between processes based on "solely automated processing," "human reviewed automated processing" and "human involved automated processing." Companies must designate a way for consumers to opt out of profiling decisions that "produce legal or similarly significant effects" if such decisions are made through automated processing. They must also provide consumers with a notice that includes a plain-language explanation of the logic used in the profiling process and disclose whether the profiling system was evaluated for accuracy, fairness or bias. A company may deny a consumer's request to opt out of profiling if the newly defined "human involved automated processing" was used. If so, instance notice with further details must be provided to the consumer.

Data Protection Assessments

Where a processing activity presents a "heightened risk of harm" to Colorado consumers, the CPA requires companies to conduct a "data protection impact assessment" (DPIA). A DPIA must be a "genuine, thoughtful analysis" that covers all aspects of a controller's organization structure. The Draft Rules list 18 topics that must be included in the DPIA, including the specific purpose of the processing, procedural safeguards, names and categories of third-party recipients of personal data and risks to consumers. These DPIAs must be revisited and updated regularly – and at least annually with respect to certain profiling decisions.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Eric Gordon, an attorney at Davis+Gilbert, assisted with this alert.