DAVIS GILBERT

Privacy + Data Security

Revised Colorado Privacy Act Rules

The Bottom Line

- While companies are working to update their privacy notices and internal practices in light of the new California and Virginia laws that went into effect on January 1, 2023, they should consider additional issues covered by Colorado's law.
- Colorado's rules are not yet final, so we can expect changes before the statute's effective date on July 1, 2023.

The Colorado Attorney General's Office released proposed revised rules (Revised Rules) governing the Colorado Privacy Act (CPA) at the end of last year. The AG's Office is accepting public input on specific topics and will hold a rulemaking hearing on February 1, 2023 to address the revised changes and additional public feedback. Final rules are expected before the CPA becomes effective on July 1, 2023.

In an earlier alert, we covered the basics of the CPA and its effect on businesses. Summarized below are the most significant changes in the Revised Rules.

Privacy Notices

The Revised Rules eliminate the purpose-centric requirement for privacy notices. Now, rather than providing specific disclosures for each purpose, controllers need only connect the processing purpose with the categories of personal data processed in a way that provides consumers a "meaningful understanding" of how their data will be used. This is a positive change that facilitates harmonizing Colorado law with the California Privacy Rights Act (CPRA).

Businesses must still notify consumers of substantive or material changes to their privacy notices, such as changes to categories of personal data processed, processing purposes, sharing data, and consumer privacy rights. Additionally, when processing personal data for a "secondary use" that differs from the originally-disclosed use, controllers must now obtain new consent from consumers before processing such previously-collected data.

Consent

The CPA requires consent to process a consumer's sensitive data. Businesses may rely on valid consent obtained prior to July 1, 2023 to continue to process a consumer's sensitive data collected before that date. Businesses that do not have valid consent prior to July 1, 2023 to process such previously-collected sensitive data have until January 1, 2024 to obtain the required consent. Importantly, there is no such grace period for obtaining valid consent to process sensitive data collected for the first time after July 1, 2023.

However, sensitive data inferences may be processed without consent if, among other requirements, such inferences are deleted within 24 hours of processing. Even with this "consent-free" limited processing, a controller must still disclose the sensitive data inferences at issue, along with relevant details of its data retention and deletion policies, in a Data Protection Assessment.

Consumer consent must be "refreshed" when (1) a consumer has not interacted with the controller in the last 12 months **and** (2) the controller is processing sensitive personal data or is processing personal data for a secondary use that involves profiling that could have a significant effect on the consumer (such as decisions around financial, insurance, educational or healthcare matters).

Opt-Out Signal/Provider Compliance

The AG's Office will publish its initial list of approved Universal Opt Out Mechanisms (UOOMs) by January 2024. UOOMs are automatic signals sent by a user's browser indicating that they do not want to be tracked. Fortunately, businesses have six months from the date the AG's Office recognizes a UOOM to begin complying with it. Notably, the Revised Rules delete the provision that would have permitted a "do not sell" list to operate as a UOOM.

Data Protection Assessments

The Revised Rules substantially reduce information that controllers must include in their data protection assessments, but do add new considerations to address, such as the reasonable expectations of consumers, sources of personal data, and technology to be used in processing. This is generally good news for controllers because most of these changes streamline the data protection assessment process. Moreover, a data protection assessment undertaken under another jurisdiction's laws or regulations is now deemed sufficient if it is "reasonably similar in scope and effect."

Definitions

Since these new privacy laws are often driven by their unique, and often conflicting, definitions, it makes sense to focus on a few under the Revised Rules:

- To be deemed a "Biometric Identifier," the data generated from a person's biological, physical, or behavioral characteristics must now be such that it can be processed "for the purpose of uniquely identify[ing] an individual."
- The definition of "Publicly Available Information" now omits "[i]nferences made exclusively from multiple independent sources of publicly available information." Accordingly, such inferences must be considered personal data, even when generated from publicly available information.

Consumer Rights

Among the most notable changes to consumer rights, consumers are now entitled to receive "final Profiling decisions, inferences, derivative data, and other Personal Data created by the Controller which is linked or reasonably linkable to an identified or identifiable individual" when they make access requests. Businesses must also "avoid incomprehensible internal codes" in responses to access requests. These changes may create a considerable burden on controllers when responding to access requests. Equally important, the "impossibility" exception, which allowed controllers to explain why complying with an access request was impossible, has been eliminated.

What Hasn't Changed?

Despite the changes outlined above — and many others in the Revised Rules — certain essential provisions remain unchanged. For example, the Revised Rules still:

- Contain detailed disclosure requirements regarding bona fide loyalty programs
- State that controllers should create and enforce document retention schedules
- Contain purpose specification and secondary use obligations
- Recognize the new category of sensitive data inferences
- Set forth specific guidance about obtaining user consent
- Require detailed data protection assessments under particular circumstances
- Provide the right to opt out of profiling.

These elements of the Revised Rules preserve the significant and, in some instances, unique features of the CPA in the evolving U.S. privacy law arena.

For More Information

Please contact the attorney 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.