Insights: Alert

Colorado’s New Comprehensive Privacy Law: a Downhill Effort for the For-Profit Sector. But, Non-Profits, Welcome to the Slopes!

July 9, 2021

Written by **Vita E. Zeltser, John M. Brigagliano**

The California Consumer Privacy Act (“CCPA”) and Virginia's Data Protection Act (“CDPA”) have created a snowball effect, encouraging Colorado to be the third state to enact comprehensive data privacy legislation. On July 7, Colorado governor Jared Polis signed the Colorado Privacy Act (the “CPA”) into law.

The CPA will take effect July 1, 2023, which will be six months after the California Privacy Rights Act (an update to the CCPA) and the CDPA become effective. Companies should hop on the compliance lift by (1) determining whether their company is subject to any of these new laws, and (2) deciding if their company can harmonize high-level positions across such laws; e.g., controller/processor distinctions, or whether their company sells personal data. If compliance positions across several of these new laws can be harmonized, compliance with the CPA should be “coming home to a place you've never been before.” Companies should also streamline compliance work by simultaneously updating privacy documents, e.g., data protection agreements and privacy notices, for all three laws.

Although the CPA has some unique aspects that are noted below, there are a few reasons why many businesses who are already subject to the other U.S. data privacy laws should find compliance with the CPA smooth-shredding:

- **Limited Applicability:** A company that is subject to the CCPA should not assume that the company is also subject to the CPA. The CPA applies only to entities that conduct business in Colorado and/or target goods or services to Colorado consumers, and: 1) control or process personal data of at least 100,000 Colorado consumers per calendar year and/or 2) and derive revenue or receive a discount on the price of goods or services from the sale of personal data and control or process the personal data of at least 25,000 Colorado consumers at any given time. The CPA's applicability is strikingly different from the CCPA in a couple of ways. The CPA defines “consumers” as Colorado residents acting for household or individual purposes, whereas that term is defined much more broadly under the CCPA. The CPA, unlike the CCPA, lacks a revenue-based applicability threshold. Therefore, companies that are subject to the CCPA only by meeting the CCPA's revenue threshold may not be subject to the CPA. Moreover, the CPA's adoption of the traditional definition of “consumer” means that a much more limited set of personal data

counts towards meeting the “processing volume” applicability threshold under the CPA compared with the CCPA.

- **No Private Right of Action and Cure Period:** Like the other comprehensive privacy laws (with a limited exception), the CPA does not provide a private right of action, but is enforced by the Colorado Attorney General or a District Attorney. In addition, until January 1, 2025, prior to any enforcement action, the Attorney General or District Attorney must issue a notice of violation to the controller if a cure is possible. The Colorado Attorney General or a District Attorney may bring an action only if the controller fails to cure the violation within 60 days after receipt of the notice of a violation. Non-compliance with the CPA is considered a deceptive trade practice, which under Colorado law can result in fines up to $20,000 for each violation and a total of $500,000 for a series of related violations.

- **Exemptions for Employee and Business-to-Business Data:** The CPA specifically excludes an individual acting in an employment or commercial context from its definition of “consumer.” In addition, the CPA does not apply to “data maintained for employment records purposes.” Therefore, like the CDPA (and, generally speaking, the CCPA), the CPA does not apply to the processing of data in an employment or business to business context.

- **Similar Data Subject Rights:** Companies subject to the CCPA need not navigate new slopes for responding to data subject rights requests. The CPA has similar data subject rights to the CCPA and the CDPA, which include the right to access, correct, delete, and opt out of the sale, collection, and use of personal data. Like the CDPA, under the CPA, the consumer has the right to opt out of the processing of personal data for targeted advertising and the sale of personal data. Consistent with the CCPA and the CDPA, controllers have 45 days to respond to consumer requests.

- **Comparable Compliance Obligations:** Ultimately, the CPA requires companies to take similar compliance steps as they have taken with previous data privacy legislation. If not already done, this includes updating the company's privacy policy to include the categories of personal data collected or processed, the purposes for which personal data is processed, how consumers may exercise their rights, the categories of personal data shared with third parties, and the categories of third parties such data is shared with. Companies should update their data mapping to ensure they are processing personal data according to purpose limitations and to avoid inappropriate secondary use. Just as under the CDPA, businesses must obtain a consumer's consent for processing sensitive data, and consent must be given by a clear, affirmative act (although exceptions to the CPA, such as for fraud prevention, may mitigate that burden). For activities that present a heightened risk of harm to a consumer, companies must conduct and document a data protection assessment. Finally, any data processing contracts should be updated, as similar to the CDPA, the CPA requires that the contract contain certain processing instructions, which include the nature and purpose of the processing, the type of personal data subject to processing, the opportunity to object to subcontractors, and the implementation of appropriate technical and organizational measures.

The following are some key unique aspects of the CPA:

- **Opt-Out Mechanisms:** The CPA is unique from other U.S. data privacy legislation in that by July 1, 2023, the Attorney General is required to adopt rules detailing specifications for a universal opt-out mechanism

for sales and processing for targeted advertising. In addition, the CPA allows consumers to exercise their opt-out rights via authorized third parties. The CPA also contemplates such third parties sending opt-out requests through automated means such as a web link, browser setting, browser extension, or global device setting, which may lead to an avalanche of requests.

- **Inclusion of Non-Profits:** The CPA also differs from the CCPA and CDPA by more expressly applying to non-profit organizations. Therefore, non-profits meeting the applicability requirements of the CPA, e.g., doing business in Colorado and annually processing the personal data of 100,000 Colorado consumers, must update privacy compliance programs.

Overall, CPA compliance should be an easy trip down the slopes for most companies who have already or are in the process of adjusting their businesses to comply with previously enacted U.S. privacy laws. However, businesses should pay attention to and continue to monitor the CPA's unique details and features, such as opt-out mechanisms, to be sure that they do not crash and fall.

Related People

Vita E. Zeltser

t 404.685.6713

vzeltser@ktslaw.com

John M. Brigagliano

t 404.815.6135

jbrigagliano@ktslaw.com