Articles + Publications | October 4, 2021

New Privacy Laws From Coast to Coast: Comparing California, Virginia and Colorado

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox

In 2023, new consumer privacy laws will be effective in Colorado, Virginia, and California. Of these, the Colorado Privacy Act (SB 21-190, the "CPA") is the latest to be enacted. Effective July 1, 2023, the CPA shares many terms and concepts with the California and Virginia laws. The Colorado law borrows more heavily than the others from the General Data Protection Regulation of the European Union (the "GDPR") in terminology, consumer rights, and the requirements of controllers (as defined below). Colorado also takes a new approach to enforcement, but with a long 60 day cure period that offers controllers an opportunity to fix issues before facing penalties. At the end of this article is a summary chart, comparing the California, Colorado and Virginia privacy laws. We note that the California Consumer Privacy Act is currently in effect, but the comparisons below and the summary chart consider the California and Virginia laws as of January 1, 2023, when the California Privacy Rights Act ("CPRA") and Virginia ("VCDPA") privacy laws become effective.

The CPA applies to "controllers," defined to include persons that determine the purposes for and means of processing personal data and that (i) conduct business or produce goods or services that are intentionally targeted to Colorado residents, and (ii) either: (A) control or process personal data of more than 100,000 Coloradans per year; or (B) derive revenue from the sale of personal data of at least 25,000 Coloradans. Unlike California, the Colorado law (similar to the Virginia law) does not include the total revenue threshold that exists in California. Although Colorado does not include a broad exemption for non-profits, there are exemptions for state institutions of higher learning that maintain personal data for non-commercial purposes. Like Virginia, Colorado defines "consumer" to exclude both the information of personnel (including employees), and business contacts. In California, the personnel and business to business exemptions are currently scheduled to sunset on January 1, 2023. Many of the CPA's exemptions follow those in Virginia, which differ from California. For example, financial institutions subject to the federal Gramm-Leach-Bliley Act of 1999 (the "GLBA") are exempt from the Colorado and Virginia statutes; only data collected subject to the GLBA (rather than the institutions themselves) are exempt from the CPRA.

The consumer rights provided by the CPA are similar to the rights provided under the California and Virginia statutes. It affords rights of access, correction, portability and deletion, as well as rights to limit processing and to opt out of sales of data, profiling and targeted advertising. If Coloradans believe their rights are not being respected, they also have the right to appeal a controller's determination, similar to the Virginia right to appeal. As in the GDPR, VCDPA, and CPRA, Colorado also requires controllers to enter into contracts with processors, which are defined as third parties that process personal data on the controller's behalf, and to provide reasonable data

security.

The CPA does contain some requirements, such as the requirement to perform Data Protection Assessments ("DPAs"), that will be new to many controllers that do not already process sensitive personal data under the GDPR. A DPA will be required prior to performing certain processing activities considered "high risk". This includes processing of "sensitive data," which includes health data, genetic or biometric data, children's data, or data that would reveal an individual's race, ethnicity, sexual orientation, sex life, or citizenship status. DPAs will also be required for targeted advertising or profiling if the processing could result in wide variety of otherwise reasonably foreseeable risks to Coloradans following the processing activities. Sales of personal data will also require a DPA. Although the new Colorado requirements to conduct DPAs are similar to the current GDPR requirements, these requirements are new on the U.S. privacy landscape, and will be the largest adjustment in terms of internal processes for controllers already used to many of the types of requirements such as contracting, reasonable security, and consumer rights management that already exist in California.

The CPA delegates enforcement to the Colorado Attorney General and District Attorneys, while the Attorney General will be responsible for enforcement in Virginia, and the new California Privacy Protection Agency will be charged with enforcing the CPRA. Colorado also raises the maximum penalty amounts compared to California and Virginia from $7,500 to $20,000 per violation. Colorado does, however, adopt two business-friendly provisions related to enforcement. First, like Virginia's law and unlike California's, the CPA does not incorporate a private right of action, which allows controllers to avoid the uncertainty of class actions and other private litigants stemming from this law. Second, the CPA provides for a 60 day cure period following a violation before penalties may be sought, in contrast to Virginia's 30 day cure period. (It is worth noting that the current 30 day right to cure under the California law will be removed by the CPRA with respect to enforcement actions, leaving a 30 day right to cure only for private rights of action as of January 1, 2023.) The CPA's right to cure will help controllers as they adjust to the new law and many of the new requirements.

The following chart offers a summary and comparison of the features of the California, Virginia and Colorado statutes:

Topic	California	Virginia	Colorado

		more than half of gross revenues from the sale of personal data.	receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.
Applicability Personal Information or Personal Data *[Different thresholds for applicability]* *[Similar definitions in CA, CO and VA.]*	For profits that do business in CA, meeting one of three thresholds: 1. Revenues over $25,000,000; 2. Collect personal information of over 100,000 consumers or households; or 3. Generate at least half of revenues from sales of personal information.	Persons that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that: 1. Control or process personal data of at least 100,000 consumers per year; or 2. Control or process personal data of at least 25,000 consumers and derive more than half of gross revenues from the sale of personal data.	Controller that conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado and: 1. Controls or processes the personal data of 100,000 consumers or more during a calendar year; or 2. Derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.
Sensitive Information *[Different definitions. CO and VA track the GDPR; CA also includes information that could be used to commit fraud and identity theft.]*	Sensitive personal information means (in summary) personal information that reveals certain information about a consumer. The specific categories of sensitive personal information are listed in the statute and include data types similar to those listed in Virginia and Colorado, and information such as Social Security number, driver's license, state identification card or passport numbers, account log-in, financial account, debit card or credit card numbers in combination with any required security or access code, password or credentials allowing access to an account, and precise geolocation.	Sensitive data means a category of personal data that includes data revealing racial or ethnic origin, religious beliefs, physical or mental health diagnosis, sexual orientation, or citizen or immigrant status, as well as processing of genetic or biometric data for identification, precise geolocation data, and personal data collected from a known child.	Sensitive data means personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, a person's sex life or sexual orientation, citizenship, or citizenship status, as well as genetic or biometric data that may be processed for the purpose of uniquely identifying an individual. The definition also includes personal data from a known child.

	2. Institutions and information subject to HIPAA 3. Data regulated by FCRA, DPPA, FERPA and others 4. Non-profit organizations	5. Data regulated by FCRA, DPPA, FERPA and others 6. Non-profit organizations	5. Data regulated by FCRA, DPPA, FERPA and others 6. Data maintained by state institutions of higher learning for non- commercial purposes
Key Exemptions (non- exhaustive)	*[Note: The Personnel and B2B exemptions in CA are scheduled to sunset January 1, 2023, although many expect they will be extended.]* 1. Information (not institutions) subject to GLBA or California financial privacy laws	1. Institutions subject to GLBA and its implementing regulations 2. Institutions and information subject to HIPAA 3. Personnel data 4. B2B information	1. Institutions subject to GLBA and its implementing regulations 2. Institutions and information subject to HIPAA 3. Personnel data 4. B2B information
Consumer Rights			
Right of Access	Yes	Yes	Yes
Right of Portability	Yes	Yes	Yes
Right to Correct	Yes	Yes	Yes
Right to Delete	Yes	Yes	Yes
Opt-out Right (Ads / Selling)	Yes	Yes	Yes
Opt-in Right for processing Sensitive Data	No (Although may limit use and sharing)	Yes	Yes
Non-Discrimination Right (for exercising consumer rights)	Yes	Yes	No
Private Right of Action	Yes	No	No
Business/Controller Obligations			
Notice to Consumers	Yes (Notice at Collection specifically required)	Yes	Yes
Privacy Policy	Yes (California Privacy Policy specifically required)	No (although required disclosures may be incorporated in privacy policy)	No (although required disclosures may be incorporated in privacy policy)
Contractual Requirements for Third Party Service Providers/ Processors	Yes	Yes	Yes
Data Processing Impact Assessments (DPAs)	No	Yes	Yes
Enforcement			
Right to Cure	None (Note: existing right to cure sunsets January 1, 2023)	30 days	60 days
Enforcer	Dedicated enforcement agency (CPPA), Attorney General, and	Attorney General	Attorney General and District Attorneys

	Private litigants		

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber