Articles + Publications | January 24, 2022

Evolving Privacy Requirements in the U.S.: What to Do for 2022?

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox | Niya T. McCray

Addressing the evolving landscape of privacy laws will be at the top of the list of New Year's resolutions for those doing business in the U.S. Businesses will need to assess and address changes in California privacy law, and new privacy laws in Colorado and Virginia, all to be effective in 2023, and to track the developments in other states. Initially, businesses must make the threshold assessment of applicability. From there, businesses will need to address the new substantive requirements, develop required disclosures, implement required practices, update vendor contracts, and train their workforces for the changes to come.

California, Virginia and Colorado are only the tip of the iceberg. Given that most states have some form of consumer privacy legislation at some stage of study, proposal or consideration, businesses can expect other states to enact new consumer privacy legislation. Businesses that may be subject to two or more of these laws should start making decisions about overlaps and conflicts in the compliance effort. Can disclosures, consumer rights and obligations imposed by California, Virginia and Colorado (and eventually other states) be coordinated and consolidated across jurisdictions? Should they be extended to consumers in other jurisdictions? Businesses will take different approaches to compliance, but all of them must focus early in 2022 on satisfying the requirements with imminent effective dates.

I. CPRA

In California, the California Privacy Rights Act ("CPRA") is essentially an amendment to the existing California Consumer Privacy Act ("CCPA"). Most provisions of the CPRA become effective January 1, 2023, but businesses will need to take action in 2022.

The CPRA applies to for-profit businesses doing business in California that meet one or more of the statutory thresholds: (i) gross annual revenues over $30 million; (ii) half of revenues from sales of personal information; or (iii) collection of personal information from more than 100,000 California residents or households. Businesses that meet any one of these thresholds must prepare in 2022 to comply with the CPRA requirements to be effective January 1, 2023.

For businesses subject to the CPRA, the following is a recommended action plan for 2022:

a. Examine the Applicability of Available Exemptions. Even if the business determined that exemptions from the CCPA applied, CPRA exemptions should be considered carefully. For example, the CCPA threshold based on revenues was increased by the CPRA, and a business currently subject to CCPA compliance may be exempt

under the CPRA.

b. Revisit and Confirm Compliance with CCPA. As the CPRA represents amendments to the CCPA, the first step in preparing for CPRA compliance is to revisit and confirm key components of CCPA compliance. This means confirming and updating where necessary the CCPA privacy policy and notice at collection, as well as the internal processes, checklists and forms for responding to consumer requests under the CCPA.

c. Prepare to Extend Disclosures, Consumer Rights and Obligations to Personal Information Subject to Sunsetting CCPA Exemptions. The important (although limited) CCPA exemptions for personal information collected from personnel (i.e., employees, contractors, job applicants, officers and directors) are scheduled to sunset January 1, 2023. Therefore, such personal information collected must be tracked and preparations must be made to treat all such data as subject to the CPRA.

d. Consider and Track Sensitive Personal Information, a New CPRA Category of Personal Information. The CPRA introduces a new category of personal information, "sensitive personal information," which includes a new consumer right to limit use, and new disclosure obligations.

e. Update Disclosures, Forms and Checklists. Starting with the CCPA compliance set, focus on implementing the changes for CPRA compliance. These include disclosures of the new consumer rights to be granted by the CPRA: the right to correct inaccurate personal information, and the right to limit the use and disclosure of sensitive personal information. The CPRA may also necessitate changes and adjustments that will need to be made to disclosures of existing CCPA rights, and to respond to related consumer requests.

f. Track Data subject to New CPRA Consumer Rights. The new consumer rights granted by the CPRA become effective on January 1, 2023, but apply to data collected during the prior 12 months. Therefore, businesses must track the data collected during 2022, including the systems where the data are processed and the third parties, service providers, and contractors with which it is shared, so that they can comply with and respond promptly to consumer requests received on and after January 1, 2023.

g. Amend Contracts with Third Parties, Service Providers and Contractors to meet CPRA requirements. Given that CPRA contains new contracting requirements, vendors need to be assessed for their status under the CPRA and contracts must be adjusted accordingly. Specifically, contracts will need to have different language depending on the role of the vendor, whether the vendor acts as a third party, service provider, or contractor. These three terms are defined roles under the CPRA. At a baseline, any contract with a third party, service provider or contractor must: (i) limit the purposes for which personal information may be used; (ii) require vendors to comply with the CPRA with respect to the disclosed information; (iii) provide for audits of vendor compliance; (iv) require notice by the vendor of noncompliance; and (v) include rights for the business to take reasonable and appropriate steps to remediate unauthorized uses of personal information. Additional requirements exist for service providers and contractors.

II. VCDPA

The Virginia Consumer Data Privacy Act (the "VCDPA") becomes effective January 1, 2023, and like the CPRA requires action in 2022 to prepare for compliance. The VCDPA applies to persons that conduct business in

Virginia or produce products or services that are targeted to Virginia residents and that meet one of two thresholds, both of which are based on data: control or process personal data of at least (i) 100,000 consumers per year, or (ii) 25,000 consumers and derive more than half of gross revenues from sales of personal data. Exemptions under the VCDPA are often broader and institution-based, in contrast to the typically information-based exemptions of the CPRA. For example, the VCDPA exempts businesses that are subject to the Gramm-Leach-Bliley Act (the "GLBA") or the Health Insurance Portability and Accountability Act ("HIPAA"), in contrast to the CPRA, which exempts information, not institutions, subject to these statutes. Similarly, the CPRA sunsets the personnel and business-to-business exemptions, but the VCDPA defines "consumer" to apply only to residents in the consumer context, which would completely exempt information collected from personnel or business-to-business contacts.

For businesses subject to the VCDPA, the 2022 action plan includes the following:

a. Examine the Applicability of Available Exemptions. The VCDPA offers various exemptions, some similar to and some different from the CPRA. For example, unlike the CPRA, the VCDPA provides an entity-level exemption for financial institutions (and their affiliates) subject to the GLBA. VCDPA also broadly exempts HIPAA covered entities and business associates, nonprofits, and institutions of higher education. Data-specific exemptions also exist, such as information used for public health activities, Family Educational Rights and Privacy Act ("FERPA") information, and data processed or maintained for administering employee benefits.

b. Review or Implement Contracts with Processors to require Compliance with VCDPA. Controllers are responsible for maintaining written contracts with processors that perform data processing on behalf of the controller. Controllers' contracts with processors must, at a minimum: (i) subject processors to a duty of confidentiality; (ii) require that data is returned or destroyed following the processing; (iii) provide audit rights for the controller; and (iv) require processors to restrict sub-processors.

c. Prepare Disclosures, Forms and Checklists. The VCDPA includes consumer rights similar to those granted by the CPRA, and controllers should adopt the necessary policies, checklists, and consumer-facing disclosures and other forms to comply with the consumers' rights, such as those to access, correction, deletion, data portability, appeal and opt-out.

d. Track Data subject to VCDPA Consumer Rights. The new consumer rights granted by the VCDPA become effective on January 1, 2023. Therefore, businesses must prepare to track and perform data protection assessments for the applicable data planned to be collected at and after January 1, 2023, including the systems where it will be processed and the processors with which it will be shared, so that they can comply with and respond promptly to consumer or Attorney General requests received on and after January 1, 2023.

e. Amend Contracts with Processors to push down new VCDPA Consumer Rights. Given that compliance with and response to consumer requests means pushing down obligations to service providers and contractors, the new VCDPA rights require review and, where appropriate, amendment of contracts with these parties.

f. Conduct Data Processing Impact Assessment. The VCDPA requires data controllers to conduct and document a Data Protection Assessment ("DPA") in certain circumstances. A DPA is required when personal data is processed for:

i. purposes of targeted advertising;

ii. the sale of personal data;

iii. the profiling of consumers with a reasonably foreseeable risk of (1) unfair, deceptive, or disparate impact, (2) financial, physical, or reputational injury, (3) reasonably offensive intrusion upon solitude, seclusion, or private affairs, or (4) any other substantial injury; or

iv. any processing activity involving personal data that presents a heightened risk of harm to consumers.

A DPA must identify and weigh the benefits of processing to the controller, consumer, other stakeholders, and the public against the rights of and risks to the consumer.

III. CPA

The Colorado Privacy Act (the "CPA") becomes effective July 1, 2023, and like the CPRA and the VCDPA requires action in 2022 to prepare for compliance. The CPA applies to any data controller that conducts business in Colorado or produces products or services that are intentionally targeted to Colorado residents; and that meets one of two data-based thresholds: control or process personal data of at least (i) 100,000 consumers per year, or (ii) 25,000 consumers and deriving revenue or receiving a discount from the sale of personal data. Like the VCDPA, the CPA provides exemptions that are broader and institution-based, in contrast to the information-based exemptions of the CPRA. For example, CPA (similar to the VCDPA) exempts businesses that are subject to the GLBA and HIPAA, in contrast to the CPRA, which exempts information, not institutions, subject to these statutes. Similarly, like the VCDPA, the CPA defines "consumer" to apply only to residents in the consumer context, which would completely exempt information collected from personnel or business-to-business contacts.

For businesses subject to the CPA, the 2022 action plan includes the following:

a. Examine the Applicability of Available Exemptions. The CPA offers both entity-level exemptions and data-level exemptions that should be examined closely. For example, unlike the CPRA, the CPA provides an entity-level exemption for financial institutions (and their affiliates) subject to the GLBA. In contrast there is no entity-level exemption for HIPAA-regulated entities, although there is a data level exemption for protected health information subject to HIPAA. Unlike the CPRA, the CPA does not include an exemption based on annual revenues.

b. Review or Implement Contracts with Processors to require Compliance with CPA. Similar to the VCDPA, the CPA imposes data minimization requirements. Businesses should assess processor contracts to ensure that only data "reasonably necessary" for the specified purpose is collected, and that processors are required to assist in responding to consumer requests under the statute. Although processor contracts must require VCDPA compliance, an entity cannot avoid responsibility by delegating processing responsibilities to a processor.

c. Prepare Disclosures, Forms and Checklists. The CPA includes consumer rights similar to those granted by the CPRA, and businesses should adopt the necessary policies, checklists, and consumer-facing disclosures and other forms to comply with the consumers' rights to access, correction, deletion, data portability, appeal and opt-out.

d. Track Data subject to CPA Consumer Rights. The CPA, unlike the CPRA, does not incorporate a lookback period for data collection. Therefore, businesses should begin tracking the data collected on and after July 1, 2023, including the systems where it is processed and the processors with which it is shared, so that they can comply with and respond promptly to consumer requests received on and after July 1, 2023.

e. Amend Contracts with Processors to push down new CPA Consumer Rights. Given that compliance with and response to consumer requests means pushing down obligations to service providers and contractors, the new CPA rights require review and, where appropriate, amendment of contracts with these parties.

f. Conduct Data Protection Assessments. Although the CPA does not take effect until July 1, 2023, businesses should immediately determine their compliance obligations, including performing a comprehensive Data Protection Assessment, which is similar to the VCDPA DPA requirement described above.

IV. Conclusion

Within the next year, businesses will be expected to comply with new consumer privacy laws, at least in California and Virginia, and thereafter in Colorado and likely other states. Although the coming months may see legislative changes or interpretive guidance, the compliance effort must begin now. The first step is an examination of applicability and the availability of exemptions. Next, businesses should track their data collection, use and sharing practices for the data in scope of these requirements. Once the business has determined applicability and scope, the compliance effort can begin with an outline of the new applicable requirements, and a comparison of the requirements on a state-by-state basis. Because of similarities, many common processes and documents can be developed across jurisdictions, but it is unlikely that a business subject to all of these new laws will be able to take a one-size-fits-all approach. For compliance teams, 2022 will be a busy year, although those who are already subject to the CCPA or the GDPR will have a good head start.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber