CEP Magazine - November 2021
US privacy laws are increasing—is your privacy program ready?

By Marti Arvin

Marti Arvin (marti.arvin@cynergistek.com) is Executive Advisor at CynergisTek in Austin, Texas, USA.

The General Data Protection Regulation (GDPR) threw many US companies for a loop, particularly those with a global presence. But many domestic US companies quickly learned there was not much to be concerned with, as GDPR did not likely apply to them or the data they collected. However, with the advent of the California Consumer Privacy Act (CCPA), that changed.

The CCPA has been around for several years, but it was not until 2020 that the law was effective and regulations were enacted. Then California added the California Privacy Rights Act (CPRA) provisions to the compliance requirements, with an effective date of January 1, 2023.[1] Then in 2021, Virginia added the Consumer Data Protection Act (CDPA), effective January 1, 2023.[2] Colorado followed with the Colorado Privacy Act (CPA), effective July 1, 2023.[3] These laws discuss the way consumer/customer data is collected and used. Over the course of the past several years, multiple states have proposed privacy laws that have failed to pass their legislatures.

As of August 2021, five additional states had active bills at various stages of the state's legislative process (Massachusetts, New York, North Carolina, Ohio, and Pennsylvania). In the absence of a federal privacy law, the trend for states to pass their own privacy laws will likely continue. Even if a federal statute is passed, it remains unclear if such a law would preempt some or all of the provisions of various state laws. This means compliance and privacy professionals will need to review the existing laws and monitor those of other states to assess their compliance obligations. The first step is to understand the applicability of the laws to the organization and the personal information the organization collects from individuals. The second step is to determine the compliance steps necessary to meet the organization's legal obligations.

Understanding the provisions of state privacy laws

This will require privacy and compliance professionals to stay on top of the legal requirements associated with the data collected by their organizations. There are several initial questions that need to be asked.

- Is the law applicable to the organization? Is there an exemption for the organization?
- Is the law applicable to the data the organization collects? Is there an exemption for some categories of data the organization collects?
- What are the obligations to protect the data?
- What are the rights given to consumers/customers?

Is the law applicable?

Careful review of the provisions of each law and corresponding regulations needs to be done to determine if the

law is applicable to a particular organization. For example, the CCPA is only applicable to for-profit entities that meet one of the following criteria: an annual revenue in excess of $25 million dollars; annually buys, receives, sells, or shares personal information of 50,000 or more consumers, households, or devices; or derives 50% or more of its annual revenue from selling consumers' personal information (PI).[4] The CPRA changes these criteria slightly. It changes the criteria to say if the entity buys, sells, or shares the personal information of more than 100,000 consumers or households.[5] The annual gross revenue floor and the percentage of annual revenue derived from selling or sharing PI remain the same.

By comparison, the Virginia CDPA, similar to the CCPA, is not applicable to nonprofits.[6] The CDPA is applicable to persons that conduct business in Virginia or targets its product or services to Virginia residents if it also annually controls or processes the data of at least 100,000 consumers and controls or processes the data of 25,000 consumers and more than 50% of its gross revenue is from the sale of personal data.[7]

The CPA does not exclude nonprofits.[8] The CPA is applicable to a controller who conducts business in Colorado or produces or delivers commercial products or services that intentionally target Colorado residents and controls or processes the personal data of 100,000 or more consumers in a calendar year; or gets revenue or a discount on the price of goods from the sale of PI that processes or controls the data of 25,000 or more consumers.[9]

Is there an exemption?

Each of the laws in question have exemptions either for the type of entity or the type of data that is covered. The CDPA does not apply to state government entities, nonprofit entities, institutions of higher education, financial institutions subject to the Gramm–Leach–Bliley Act (GLBA), and entities subject to HIPAA either as a covered entity or a business associate.[10] The CPA is not applicable to financial institutions subject to GLBA,[11] nor is protected health information (PHI) under HIPAA or data collected under a program subject to the Substance Abuse and Mental Health Services Administration.[12] The CCPA is not applicable to medical information that is subject to the California Confidentiality of Medical Information Act, PHI subject to HIPAA, or information subject to GLBA.[13]

So the questions for compliance and privacy professionals are: Is your organization even covered by the particular act, and if it is, is some or all of the data the organization collects covered by the act? If the answers to those questions are yes, then considerations for obligations around appropriate protections for the data need to be considered as well as meeting requirements for the rights granted to individuals under the applicable law.