protiviti®
Face the Future with Confidence

Virginia Becomes the Second State to Enact Consumer Privacy Law

March 3,
2021

The Commonwealth of Virginia passed the Consumer Data Protection Act (CDPA) into law on March 2, 2021, following overwhelming bipartisan support for a state consumer privacy law. The November 2020 election results provided the much needed impetus to strengthen consumer privacy for the Commonwealth of Virginia. State officials wasted no time in introducing the privacy bill. Now that the bill is enacted, Virginia becomes the second U.S. state behind California to institutionalize a comprehensive consumer privacy law for businesses to govern, control and lawfully process personal information of Virginia's residents. The law goes into effect on January 1, 2023.

This Flash Report cites and summarizes key requirements contained in the new law, along with notable takeaways.

The Scope of the CDPA and What Constitutes "Personal Data"

The CDPA applies to all persons who conduct business in the Commonwealth and either control or process personal data of at least 100,000 consumers or derive over 50% of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers. The law outlines responsibilities and privacy protection standards for both data controllers and data processors.

Within the context of the law, "personal data" means any information that is linked or reasonably associated to an identified or identifiable natural person who is a resident of the Commonwealth of Virginia. According to the text, personal data does not include de-identified data or publicly available information. Further, the law introduces "sensitive personal data" as a category of personal data, and includes the following types of data under this section:

- Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.

- The processing of genetic or biometric data for the purpose of uniquely identifying an individual.
- The personal data collected from a minor.
- Precise geolocation data.

Important Provisions

Consumer Rights

The law affords Virginia residents the following five consumer rights similar to the California Privacy Rights Act (CPRA):

- Right of access to personal data.
- Right to obtain personal data in a portable and readily usable format.
- Right to correct inaccuracies in personal data.
- Right to erasure of personal data collected.
- Right to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data or auto-profiling or auto-decisions.

A business must respond to consumers within 45 days of receipt of a request submitted based on the methods described in the law. However, under certain circumstances, an extension may be granted based on the complexity of the consumer request.

Business Considerations

Transparency, Accountability and Security Requirements

The law provides a variety of requirements for data controllers:

- Controllers must limit collection and processing of personal data to what is necessary for business purposes.
- Businesses must provide consumers with affirmative consent in order to collect or process personal data.
- Should a consumer decide to exercise certain rights or opt out of processing/sharing of their data, businesses must not discriminate against the consumer for choices made by denying products or services, applying different pricing models or providing substandard quality of service to the consumer.

- Businesses collecting personal data should provide consumers with a privacy notice clearly outlining the purpose of collection and processing of personal information, the categories of data processed, and directions on how a consumer can exercise the rights provided in the text.
- Similar to the CPRA, the CDPA sets higher standards related to sale of personal data, targeted advertising and auto-profiling. The law requires businesses to provide transparent disclosure of such processing activities and the rights consumers have to opt out.
- Businesses must implement and maintain reasonable security practices to protect the confidentiality, integrity and accessibility of personal data.
- Specific to data processors, data processing activities must be governed through legally binding contracts that lay out express data protection and handling provisions.

As a recommendation, organizations should take proactive steps to update their existing business practices in the areas of privacy and data governance. Additional consideration should be given to identifying technical solutions to support data inventory and discovery processes in addition to enabling consumer rights at scale.

Data Protection Assessment (DPA)

The law provides specific directions to be followed and required criteria to be applied for conducting Data Protection Assessments. This is the first U.S. commercial requirement to require a DPA similar to the Data Protection Impact Assessment (DPIA) requirements outlined in the General Data Protection Regulation (GDPR). A business is required to conduct a DPA if the collection of personal information involves usage of targeted advertising, use of automated profiling or application of inferences made through personal data, involves processing of sensitive personal data, and if processing of personal data heightens the risk of harm to consumers.

Exemptions

The law exempts entities that are required to comply with certain sectoral laws such as financial institutions that are subject to the Gramm-Leach-Bliley Act (GLBA), healthcare sectors identified as covered entities or business associates pursuant to the Health Insurance Portability and Accountability Act (HIPAA), as well as several additional federal acts. However, entities should carefully assess the applicability of provisions to data that may fall outside of these exemptions.

Violations and Enforcement

The Virginia consumer privacy law does not provide the basis for a private right of action for residents of Virginia, which is a notable difference from the California Consumer Privacy Act (CCPA) and CPRA. Instead, the CDPA gives exclusive rights to the Virginia Attorney General to bring enforcement actions and introduces the Consumer Privacy Fund to facilitate funding efforts behind enforcements. Similar to the CPRA, if a business is found violating the requirements of the law, they will be provided with a 30-day remediation window to cure infractions. If, within this window, remediations or necessary actions are not taken, the Attorney General can seek damages of up to $7,500 per violation.

California and Virginia are the first states creating a national impact by enacting privacy laws in the absence of an overarching federal privacy law to govern data privacy. We will likely see a busy year with more states speeding up to meet the standards of California-style privacy laws.

Businesses that have made changes within their organization to comply with the California privacy laws will find it easier to align with the CDPA, although there are specific nuances to be considered for the Virginia privacy law.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of *Fortune* 1000 and 35% of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How Protiviti Can Help

Protiviti has partnered with clients across industries to stand up strategic data privacy programs, governance structures and technology implementation efforts, and to operationalize privacy processes to assist with regulatory expectations. In that spirit, we will continue to monitor and report on changes to the CDPA, contrast similarities and differences with the CCPA and CPRA as CDPA develops, and support companies on their compliance journey to meet regulatory expectations.

Our privacy consultants bring deep expertise in regulatory requirements and privacy strategy implementation, and can:

- Assess organizational privacy risks and conduct assessments using best-of-breed privacy frameworks.
- Define long-term privacy objectives and the strategic plans to implement and operationalize privacy practices.
- Assess compliance with regulatory obligations, providing gaps and remediation roadmaps.
- Conduct independent assessments of privacy programs, including policies and procedures impacting data collection, minimization and storage limitation.
- Provide guidance for Privacy by Design implementation, Data Subject Access Requests, Privacy Impact Assessments and Data Protection Impact Assessments.
- Develop sustainable processes to manage record of processing activities, data inventories and data flows.
- Evaluate vendor-risk programs and safeguards.
- Provide legal support in understanding data transfer mechanisms.

Please contact us to discuss what these new rules and regulations mean for your organization.

protiviti®