Virginia Consumer Data Protection Act to Become Effective January 1, 2023

By: Carmelle F. Alipio & Courtney Reigel

12.27.2022

Beginning in January 2023, covered businesses in Virginia will have new compliance obligations under the Virginia Consumer Data Protection Act (CDPA) in response to the new privacy rights granted to residents of the Commonwealth. Last year, Virginia became the second state after California to pass comprehensive data privacy legislation. California had previously enacted the California Consumer Privacy Act (CCPA), which became effective on January 1, 2020. Also of note, California?s new data privacy law, the California Privacy Rights Act (CPRA), which amends and expands the CCPA, also becomes effective on January 1, 2023.

The CDPA applies to for-profit individuals and entities that conduct business in the Commonwealth or produce products or services that target Virginia residents, and that, during a calendar year: (1) control or process personal data of at least 100,000 Virginia consumers, or (2) control or process personal data of at least 25,000 Virginia consumers and derive over 50 percent of their gross revenue from the sale of personal data. The CDPA provides Virginia consumers with rights relating to their ?personal data,? including the right to access, correct, and delete the personal data collected from them by a covered business. The new law also requires that covered businesses provide a mechanism for consumers to opt-out of the sale of their personal data, as well as the use of their personal data for targeted advertising or profiling purposes. The CDPA broadly defines ?personal data? and includes a sub-category of personal data that is more highly protected, called ?sensitive data,? that requires covered businesses to obtain a consumer?s opt-in consent prior to processing such data. The law also requires that certain covered businesses post reasonably accessible, clear, and meaningful privacy policies that include specific information about the business?s privacy practices. Further, covered businesses must maintain reasonable security practices to protect the confidentiality, integrity, and accessibility of personal data. In some circumstances, businesses must also conduct and document data protection assessments under the CDPA, and the Virginia Attorney General may request that a business make such assessments available for purposes of policing compliance. As a result, businesses that collect, use, share, or sell Virginia residents? personal data should closely review the CDPA to determine if they are subject to the new law.

In addition, businesses that conduct business in California and collect, use, share, or sell Californians?

personal information should carefully review the CPRA to see if they are subject to the new law, taking into consideration changes from the CCPA, and should familiarize themselves with any additional obligations. For example, certain exemptions that businesses enjoyed under the CCPA (including those pertaining to personal information collected in the employment or b2b contexts) are set to expire on January 1, 2023 when the CPRA becomes effective. The CPRA also includes new requirements and adds, like the CDPA, a protected class of ?sensitive information? that places additional restrictions on covered businesses.

Businesses should closely monitor emerging laws as more and more states, such as Colorado, Utah, and Connecticut, pass comprehensive data privacy legislation to ensure compliance.

Stay tuned for more legal developments related to data management, including privacy and data protection, cybersecurity, intellectual property rights and data quality. Please contact Courtney Reigel or Carmelle Alipio with any questions.

Related People

- Carmelle F. Alipio ? 919.981.4038 ? calipio@williamsmullen.com
- Courtney Reigel ? 804.420.6368 ? creigel@williamsmullen.com

Related Services

- Data Protection & Cybersecurity