O'Melveny

Alerts & Publications

Virginia is for Lovers and Now It's for Lovers of Data Privacy

March 15, 2021

KEY CONTACTS

Tod Cohen
Washington, DC
D: +1-202-383-5348

Randall W. Edwards
San Francisco
D: +1-415-984-8716

Scott W. Pink
Silicon Valley
D: +1-650-473-2629

Amit Itai
Silicon Valley
D: +1-650-473-2647

Ben Seelig
San Francisco
D: +1-415-984-8947

On March 2, 2021, Virginia Governor Ralph Northam signed the Consumer Data Protection Act (VCDPA) into law, following California to become the second state to enact comprehensive consumer privacy legislation.[1] While the law is largely modeled on the California Consumer Privacy Act (CCPA) and the EU's General Data Protection Regulation (GDPR), companies doing business in Virginia should be aware of how the law differs from those regimes before it comes into effect in January 2023. Most notably, the VCDPA imposes new obligations by requiring entities that control personal data to conduct "data protection assessments" to evaluate the risks of data processing activities.

Since the passage of the CCPA in 2018 and the subsequent success of the California Privacy Rights Act (CPRA) ballot initiative in 2020, many predicted a proliferation of legislation in other states that take a similar holistic approach to regulating the use of personal data. Indeed, Nevada and Maine adopted less comprehensive privacy legislation, and 12 state legislatures have introduced or re-introduced comprehensive data privacy laws just in the first three months of 2021. Even if your business is not directly subject to the VCDPA, it is another bellwether signaling new bipartisan data privacy laws we expect to see adopted throughout 2021.

Scope

The VCDPA adopts the GDPR's terminology of "controllers" and "processors". The classifications apply to companies that control data (controllers) or process data on behalf of controllers (processors), who conduct business in Virginia or target Virginia residents with their products or services and either control or process the personal data of at least:

1. 100,000 Virginia residents (consumers) annually; or
2. 25,000 Virginia residents (consumers) and derive at least 50% of gross revenue from the sale of that data.

The statute explicitly exempts employee data, entities subject to HIPAA, as well as nonprofits, universities and colleges, and financial institutions.

Consumer Rights

The VCDPA creates a rights-based regime similar to the EU's GDPR and California's CCPA. In that vein, the VCDPA provides six specific rights for Virginia consumers:

1. the right to **access** their data;
2. the right to **correct** their data;
3. the right to **delete** their data;
4. the right to **data portability**;
5. the right to **opt-out** of certain uses of their data, including sale, targeted advertising, and other forms of profiling; and
6. the right to **appeal** a controller's decision with regard to a consumer's request to invoke the rights listed above.

The VCDPA defines "targeted advertising" as "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests." The law clarifies that this definition **does not** include:

1. Advertisements based on activities within a controller's own websites or online applications;
2. Advertisements based on the context of a consumer's current search query, visit to a website, or online application;
3. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or
4. Processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

Controller and Processor Obligations

The VCDPA requires data controllers to limit their collection of personal data that is "adequate, relevant and reasonably necessary" and in line with the privacy notice they provide consumers. A controller cannot use personal data in a manner not described in the privacy notice, unless they obtain the consumers' consent. The law also requires companies to conduct "data protection assessments" related to their processing of personal data for targeted advertising and any sale of personal information.

The "sale of personal information" is defined as "the exchange of personal data for monetary consideration by the controller to a third party," which is narrower than the definition under the CCPA. The definition of a sale of personal information excludes certain types of disclosures, including: disclosures to processors, disclosures to a third party for purposes of providing a product or service requested by the consumer, disclosures to affiliates, disclosures of information that consumers made widely available, and disclosures as part of a merger or acquisition.

The VCDPA requires that controllers provide consumers with a privacy policy that includes:

- The categories of personal data processed by the controller;
- The purpose for processing personal data;
- How consumers may exercise their right to appeal a controller's decision regarding a consumer's request;
- The categories of personal data that the controller shares with third parties; and
- The categories of third parties with whom the controller shares personal data.

Under the VCDPA, controllers and processers also must protect the data they collect or process and are required to "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data." Unlike the CCPA, however, the VCDPA does not create a privacy right of action for security breaches.

Similar to GDPR's Article 28, processors are required to follow the instructions of the controller and assist them in meeting its obligations under the law pursuant to a written agreement.

Data Protection Assessments

The VCDPA departs from the CCPA in that it requires controllers to conduct "data protection assessments." While the law specifies that certain activities must be assessed, it is silent on how often the assessments must occur, when they must occur, and for how long a controller must keep information related to the assessments.

Under the law, a controller shall "conduct and document" data protection assessments on the following processing activities:

1. The processing of personal data for purposes of targeted advertising;
2. The sale of personal data;
3. The processing of personal data for purposes of profiling, when there is a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;
4. The processing of sensitive data; and
5. Any processing activities involving personal data that present a heightened risk of harm to consumers.

This is similar in nature to "Data Protection Impact Assessments" in Article 35 of the GDPR, although Virginia's requirements are likely broader in scope than the EU's since they expand beyond merely assessing activities that are "likely to result in a high risk to the rights and freedoms" of data subjects.

Enforcement and Penalties

Like the CCPA, the VCDPA does not explicitly create a private right of action for persons aggrieved by violations of the law. Rather, the state Attorney General will be tasked with enforcing the law against companies that violate its provisions, and fail to cure violations within 30 days of receiving notice. If a violation occurs, the Attorney General may seek injunctive relieve, damages for up to $7,500 per violation, and expenses.

[1] Va. Code § 59.1-571-59.1-581.
