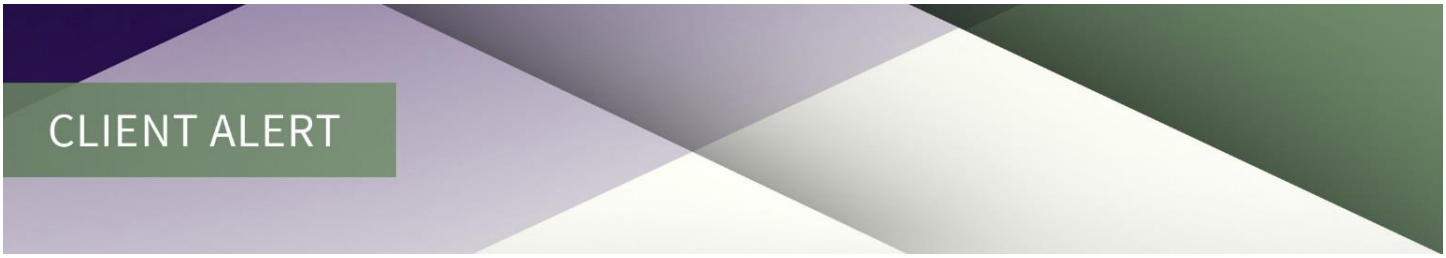

Virginia is the New Privacy Leader: What's Next After Virginia Passes Comprehensive Privacy Law

March 9, 2021

AUTHORS

Daniel K. Alvarez | Richard M. Borden | Nicholas C. Chanin

Introduction

On March 3, 2021, Governor Ralph Northam signed into law the Virginia Consumer Data Protection Act ("VCDPA"),[1] making Virginia the second state in the nation, after California, to pass comprehensive privacy legislation. The passage of the VCDPA comes on the heels of voters in California approving the California Privacy Rights Act ("CPRA"),[2] which significantly revises the California Consumer Privacy Act ("CCPA").[3] Both the VCDPA and CPRA will come into effect on January 1, 2023, giving businesses just under two years to implement necessary changes to their data collection, use, and sharing practices to bring their programs into compliance. Organizations that already have a privacy program based on the EU's General Data Protection Regulation ("GDPR") are likely to find adapting their existing programs to these laws easier than will organizations with limited or CCPA-based programs, as both the VCDPA and the CPRA hew more closely to GDPR. Still, each of these laws is sufficiently different from the others that all organizations will have some work to do to ensure compliance over the next two years.

1 Consumer Data Protection Act, SB 1392, available here.

2 California Privacy Rights and Enforcement Act, available here.

3 CAL. CIV. CODE 1798.100 *et seq.*

VCDPA: A Summary

As mentioned, the VCDPA imports a number of concepts–including certain terms and language–from the GDPR. However, in its scope and construction, it remains a largely American privacy law, with "opt-out" for collection and use of personal data (other than for "sensitive" data, to which an "opt-in" model applies). Specifically, the VCDPA:

- Applies broadly to any businesses that annually process the personal data of at least 100,000 Virginia residents, or otherwise both derive half their annual revenue from selling personal data and process the data of at least 25,000 Virginians. There are numerous exceptions in the law, such as for businesses that are subject to certain federal privacy regulations (such as HIPAA or the GLBA), where the data itself is protected by certain federal laws (such as educational records under FERPA, or credit- and background-related information governed by FCRA), and for data that is already public, has been de-identified, or is used only for employment-related purposes or in the context of business relationships;

- Grants to consumers numerous rights related to their personal data when in the hands of other parties, such as the right to have their data deleted and the right to opt-out of certain types of processing (e.g., targeted advertising or sales);

- Directs businesses to explain those rights to consumers and provide processes for exercising those rights;

- Introduces to U.S. law the GDPR's concept of "data controllers" and "data processors" and the attendant roles and responsibilities of each, including such requirements as contracts with specific data protection provisions for data processing relationships, a duty on the part of processors to assist controllers in discharging such duties as responding to consumer rights requests, and an affirmative duty on the part of controllers to implement appropriate data security practices;

- Requires data controllers, before starting certain types of processing, to perform and document a privacy assessment–similar to GDPR's data protection impact assessment–weighing the risks, benefits, and protections possible in that processing; and

- Imposes more obligations and requirements on the collection and use of sensitive data than other consumer data.

Importantly, the VCDPA does not provide a private right of action. Enforcement falls to the Commonwealth Attorney General who may bring actions against businesses for violations, seeking injunctions or fines of up to $7,500 per violation. Like the CCPA and CPRA, however, VCDPA includes a 30-day cure provision.

CPRA and VCDPA: Roommates or Hostile Neighbors?

The enactment of VCDPA at this time presents particular challenges to companies because compliance work will need to happen simultaneously with similar work for CPRA. As we discussed in a previous alert,[4] the CPRA is not merely an update to the CCPA. The changes to CCPA enacted by CPRA are significant. For instance, the CPRA (i) introduces the right of consumers to request the correction of their personal data; (ii) expands the "opt-out" right to require that businesses provide a means for consumers to "opt-out" of *any* data sharing for targeted advertising; and (iii) directs service providers to assist businesses in responding to consumer rights requests. These requirements will be new in California, and therefore new to any company whose privacy practices are solely based on the CCPA, but similar provisions were enacted with the GDPR in May 2018, and will apply in Virginia simultaneously with the CPRA in January 2023.

Work to Be Done

The two years that companies have to come into compliance with the CPRA and VCDPA may seem like a lot of time, but many companies will have a significant task ahead, not the least of which is actually identifying what specific steps the company itself must take. Some examples of likely workflows include:

- Data mapping/data flow review to understand what types of personal data are coming in, its sources, its purpose, its retention period, and who is responsible for that data and how those map to the VCDPA and CPRA requirements;
- Updating policies and procedures to ensure that employees can consistently handle consumer rights requests, data is appropriately protected, and the language in public policies and notices is common to the applicable laws;
- Identifying key data-sharing relationships and the contracts that govern them. In some cases, contracts may need to be renegotiated or amended; and,
- Redrafting, as necessary, public-facing documents to ensure those documents contain all required disclosures, and accurately reflect the company's practices.

This is likely a precursor to a busy few years for privacy and data security legislation and policymaking in the United States. First, several states appear ready to follow Virginia and California in adopting comprehensive privacy regimes: there are privacy bills in various stages of the legislative process in 12 different states.[5] Many of these laws will likely be

[4] For a more in-depth summary of the CPRA, please see Willkie's client alert from Nov. 11, 2020. Available here.

[5] *See*, IAPP TRACKER: US STATE COMPREHENSIVE PRIVACY LAW COMPARISON, https://iapp.org/resources/article/state-comparison-table/ (last updated March 3, 2021).

largely similar (for instance, the VCDPA was modeled on a bill from Washington), but as with state data breach notification laws there will probably be sufficient differences that none of these state laws can be overlooked. Second, federal privacy legislation remains a possibility, with bills coming from both Republican and Democratic legislators. Regardless of whether Congress acts, federal regulatory agencies under new leadership installed by the Biden administration appear poised to focus their energies and authority to both enforce existing privacy requirements and adopt new ones. As a result, adaptability will remain a key component of any privacy program going forward.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Nicholas C. Chanin
202 303 1164
nchanin@willkie.com