SAUL EWING ARNSTEIN & LEHR LLP

ALERT

Cybersecurity and Privacy Practice

FEBRUARY 2021

The Virginia Consumer Data Protection Act (CDPA): Key Questions and Answers

Alexander R. Bilus | Patrick M. Hromisin

Virginia is on the brink of joining California as the second state with a broad privacy law that restricts how companies can use and disclose personal information. The Virginia Consumer Data Protection Act (CDPA) recently passed both houses of the legislature and is expected to be signed into law by Governor Ralph Northam as early as next month. The bill is somewhat similar to the California Consumer Privacy Act (CCPA), which went into effect last year and prompted many businesses to examine and update their privacy programs. It also includes some concepts comparable to the European Union's General Data Protection Regulation (GDPR), but there are important differences between the CDPA and both the CCPA and the GDPR.

Below is a series of questions and answers about Virginia's CDPA to help you understand whether it applies to your company and what obligations it will place on your company.

- **Am I crazy, or does it seem like this came out of nowhere?**
  - You're not entirely crazy. It only took about three weeks for this bill to get through the commonwealth's legislature. This is in part due to broad agreement among Democrats (who control the legislature) on the bill's terms. It is also a function of Virginia's unusually brief and rapid legislative session. Some other states, most notably Washington, have been considering broad data privacy bills for years without getting them passed.
- **To whom will the CDPA apply?**
  - *Controllers*: The CDPA applies to for-profit businesses that conduct business in Virginia, control the purposes and means of processing personal data, and:
    - Control or process data for at least 100,000 Virginia residents; or
    - Make 50 percent of their gross revenue from the sale of personal data and control or process personal data of at least 25,000 Virginia residents.
  - *Processors*: The CDPA also applies to entities that process personal data on behalf of a controller, although their obligations are more limited, as discussed below.
  - As under the CCPA, non-profit organizations are not subject to the CDPA.
  - Unlike the CCPA, there is no revenue amount threshold for businesses to fall within the scope of the CDPA, so it will apply to businesses both large and small.
- **When will the CDPA go into effect?**
  - January 1, 2023.
- **What information does the CDPA protect?**
  - The CDPA will apply to "personal data," which it defines broadly as "any information that is linked or reasonably linkable to an identified or identifiable natural person."

- But like the CCPA, the CDPA does not apply to certain categories of data, including:
  - Data being processed as part of an employment relationship with an individual;
  - Data already protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA);
  - Data subject to the Gramm-Leach-Bliley Act (GLBA);
  - Data regulated by the Family Educational Rights and Privacy Act (FERPA); and
  - Data bearing on a consumer's creditworthiness where the processing of such data is regulated by and authorized under the Fair Credit Reporting Act (FCRA).

- **What are the rights granted to Virginians by the CDPA?**
  - Like the CCPA, the CDPA grants Virginia residents the right to request access to, deletion, correction, and copies of personal data.
  - It also gives Virginia residents the right to opt out of the processing of their personal data for purposes of:
    - targeted advertising;
    - the sale of personal data; or
    - profiling in furtherance of decisions that produce "legal or similarly significant effects" concerning the individual.
- **What are the obligations placed on controllers by the CDPA?**
  - The CDPA forbids businesses from collecting personal data unless that information is "adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed."
  - It also requires businesses to establish, implement, and maintain reasonable administrative, technical, and physical data security practices.
  - It requires businesses to provide consumers with privacy notices disclosing a number of features of the business' processing of personal data.
  - It prohibits businesses from processing "sensitive data" (which includes racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, as well as biometric and geolocation data) without an individual's consent, and requires such consent to be "freely given, specific, informed, and unambiguous."
  - It also requires businesses to conduct Data Protection Assessments in particular situations, including when the business is selling personal data or processing it for purposes of targeted advertising.
- **What are the obligations placed on processors by the CDPA?**
  - Companies (like service providers) that process personal data on behalf of businesses that are subject to the CDPA are required to assist those businesses in complying with their CDPA obligations.
  - Processors are also required to execute contracts with such businesses that set forth instructions for processing personal data and that restrict the ability of processors to use and disclose the data in certain ways.
- **How will the CDPA be enforced?**
  - It will be enforced exclusively by Virginia's Attorney General, and violations may be subject to a civil penalty of up to $7,500 per violation.
  - But the CDPA also provides that the Attorney General must give any alleged violator 30 days' notice and an opportunity to "cure" the violation before initiating an enforcement action.

- **Does the CDPA include a private right of action?**
  - No. Unlike the CCPA, which includes a limited private right of action for unauthorized disclosures of personal data, the CDPA creates no avenue for private lawsuits.
  - Of course, that won't strop enterprising plaintiffs' attorneys from trying to bring negligence, fraud, and other lawsuits alleging violations of the CDPA. In California, for instance, plaintiffs have sued for alleged CCPA violations that go beyond the terms of that law's private right of action.
- **If my company is compliant with the CCPA, will we be compliant with the CDPA?**
  - CCPA compliance is a good start toward CDPA compliance, but given the differences between the two laws, it's not sufficient in and of itself. Companies will need to pay particular attention to their processing of sensitive personal data and the need to perform Data Protection Assessments.
- **What are some of the key differences between the CDPA and the CCPA?**
  - The CDPA's opt-out rights include the right to opt out of not just sales of personal data (like the CCPA) but also certain profiling activities and targeted advertising.
  - The CDPA's provisions on sensitive data and consent are significantly broader and more restrictive than anything the CCPA currently requires, although the CCPA was recently amended to allow Californians to opt out of the sharing and use of sensitive personal data beginning in 2023.
  - The CDPA's requirement that businesses conduct Data Protection Assessments is unlike anything currently required by the CCPA (although it is somewhat comparable to the GDPR's requirement for Data Protection Impact Assessments and an amendment to the CCPA that will go into effect in January 2023 and will require businesses to submit to regulators risk assessments with respect to their processing of personal data).
- **Is the CDPA likely to be amended significantly before it goes into effect?**
  - Initial reports indicated limited legislative interest in making further substantive changes to the CDPA prior to enactment. But as the bill has gained more public attention, numerous organizations have called for changes. In particular, certain privacy advocates have called for the legislature to hit the "pause button" and consider adding provisions such as a private right of action and an anti-discrimination provision. Legislators have until March 1 to amend it, and the Governor has a line-item veto, which provides further opportunity to change the bill. We will provide further updates if the bill is materially altered before enactment.

Saul Ewing Arnstein & Lehr's Cybersecurity and Privacy attorneys can help your company with its CDPA compliance strategy. Contact the authors of this article for more information.

This alert was written by Alexander R. Bilus, vice-chair of the Firm's Cybersecurity and Privacy Practice; and Patrick M. Hromisin, a member of the Practice. Alexander can be reached at (215) 972-7177 or at Alexander.Bilus@saul.com. Patrick can be reached at (215) 972-8396 or at Patrick.Hromisin@saul.com.
This alert has been prepared for information purposes only.

Did you find this information useful? Please provide your feedback here and also let us know if there are other legal topics of interest to you.