Brownstein Hyatt Farber Schreck

News

March 2, 2021

New State Data Privacy Requirements Continue To Pile On

Virginia Is on the Verge of Passing Its Own Consumer Data Protection Act

California is no longer the lone state with a consumer data privacy law. Virginia is now on the verge of joining, pending a formal reconciliation between the Virginia House and Senate versions, as well as the governor's signature. The Virginia Consumer Data Protection Act (CDPA) resembles California's CCPA and Europe's GDPR in some—but not all—aspects.

Although the CDPA will not become effective until Jan. 1, 2023, companies should get their data privacy affairs in order because other states, and eventually the federal government, will likely pass their own laws, soon enough, and they may have different obligations companies should be aware of. Accordingly, now is the time for companies to familiarize themselves with the consumer data privacy requirements, or else they risk facing significant penalties down the road.

Below is a quick summary of the CDPA and some guidance for businesses to consider.

Who Does the CDPA Apply to?

The CDPA applies to a company if it does business in Virginia and if it (1) controls or processes, during a calendar year, the personal data of at least 100,000 Virginia residents, or (2) controls or processes the personal data of at least 25,000 Virginia residents, and derives over 50% of gross revenue from selling personal data.

What Does the CDPA Provide?

Similar to California's CCPA and Europe's GDPR, Virginia's CDPA creates individual rights for Virginia consumers, including (1) the right to access their data, (2) the right to amend their data, (3) the right to delete their data, (4) the right to transfer their data, and (5) the right to opt out of certain uses of their personal data. On that last point, it's noteworthy that the consumer's right to opt out does not just apply to the sale of personal data, it also applies to targeted advertising and other forms of profiling. It is also noteworthy, though not surprising, that there is no private cause of action.

What Are Companies Required to Do Under the CDPA?

Covered businesses are required to (1) adopt data minimization practices, (2) disclose their privacy practices through a "meaningful privacy notice," (3) implement data security measures, (4) refrain from discriminating against consumers who exercise their rights under the CDPA, and (5) obtain consent prior to processing sensitive data, as defined below.

Covered businesses that determine the purpose and means of processing personal data are also required to conduct risk assessments on their data protection practices. Such assessments must be taken where a data controller (1) processes personal data for targeted advertising, (2) sells personal data, (3) processes personal data to profile "where such profiling presents a reasonably foreseeable risk of" injury, or (4) processes sensitive data.

What Is "Sensitive Data" and Why Is It a Critical Part of This Law?

Sensitive data is personal data revealing racial, ethnic, religious, mental or physical characteristics about you, including genetic or biometric data, data collected from a child or precise geolocation data. This definition largely mirrors what is considered sensitive data in Europe under the GDPR. Critically, under CDPA companies must obtain consent to process sensitive data, as well as disclose collection and use of sensitive data. And this may ultimately become a source of major confusion between companies and consumers: California's recently passed ballot initiative amending the CCPA also creates a category of "sensitive data," but it is different from Virginia's CDPA. In particular, it includes Social Security numbers and drivers' license numbers. So a business's communications about privacy practices will have to distinguish between the two jurisdictions, especially where a company cannot give a choice regarding the processing of a Social Security number (where it's collected for tax or Know Your Customer reasons, for example).

What Happens If a Company Violates CDPA?

Companies that violate any CDPA provision and fail to cure within 30 days of receiving notice are subject to civil prosecution by the Virginia attorney general and may face liability of up to $7,500 for each violation. While the CDPA does not allow for a private right of action, companies should know that they can still face consumer-driven lawsuits for common law claims of invasions of privacy and statutory consumer protection actions.

Conclusion

The CDPA is the latest regulatory framework to govern a company's use of personal data. There are similarities between the CDPA and the CCPA and GDPR, but there are also certain differences. As more states adopt their own privacy laws, companies will need to respond and hope that federal action to govern this aspect of a business's operations takes place. In the meantime, companies should, at a minimum, catalog the types of personal information they collect and how it is used, update privacy policies and set up a process to timely respond to consumer requests about their data. It is highly likely that other states, and possibly the federal government, will pass data privacy laws in 2021 or 2022 with similar requirements to the CDPA, CCPA and GDPR.

Contact us for a more in-depth analysis of how your business can be prepared for the oncoming data privacy laws and regulations.

Name
Shareholder
Email
303.223.1232

Name
Shareholder
Email
303.223.1232

Name
Shareholder
Email
303.223.1232