

# PUBLICATION

---

## Privacy Legislation Floodgates Have Opened: Virginia Passes the Consumer Data Protection Act

Authors: Alexander Frank Koskey, III, Matthew George White  
February 23, 2021

Virginia has become the latest state to pass comprehensive privacy legislation as its legislature voted to enact SB 1392, known as the Consumer Data Protection Act (the "Act"). Although many other states have proposed privacy laws during current legislative sessions, Virginia becomes the first state this year to adopt new privacy legislation, which is expected to be signed by the governor within the next few weeks. The Act would take effect on January 1, 2023.

The Act is noteworthy for several reasons:

- (1) It adopts the concepts of "controller" and "processor" found in the European Union's General Data Protection Regulation (GDPR) and focuses on the "processing" of personal data of consumers;
- (2) It requires controllers to perform and document data protection assessments for specified processing activities; and
- (3) It continues the trend of expanding consumer rights, as we have seen in the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA).

The Act is going to have a substantial impact on businesses that process the personal data of Virginia consumers and is likely to create new compliance hurdles for covered businesses. Businesses that are subject to California's privacy regime may have a head start in preparing to comply with the Act but will nevertheless still need to ensure compliance with its unique provisions. Covered businesses that have not dealt with CCPA/CPRA compliance will have a significant amount of work to do. This alert summarizes several of the key provisions in the Act..

### Scope and Applicability

The Act applies to persons who conduct business in Virginia or "produce products or services that are targeted to residents of Virginia" and either:

- (i) "control or process the personal data of at least 100,000 consumers" during a calendar year

*or*

- (ii) "control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data."

"Personal data" is defined by the Act as "any information that is linked or reasonably linkable to an identified or identifiable natural person." This is similar in concept to the CCPA, but sets a different standard for organizations to absorb.

A "consumer" is defined as "a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a person acting in a commercial or employment context." This definition is significant as the Act does not apply to personal data of employees or personal data collected from individuals in the context of business-to-business transactions, both of which have created significant questions as to their ultimate treatment under California's laws.

## Consumer Rights and Compliance Obligations

Similar to other proposed legislation, the Act borrows many of its consumer rights and compliance obligations from the CCPA and CPRA. These include:

- Requiring businesses to disclose (i) the categories of personal data to be processed; (ii) the purpose for processing the personal data; and (iii) the categories of personal data that is shared with third parties;
- Giving consumers the right to opt out of the sale of personal data to third parties or the processing of personal data for targeted advertising;
- Requiring data minimization principles under which only personal data that is "adequate, relevant, and reasonably necessary" for the purposes for which the personal data is to be processed be collected;
- Requiring businesses to establish and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of personal data at issue;
- Restricting the processing of a consumer's sensitive data without obtaining the consumer's consent;
- Providing consumers with rights to (i) access personal data being processed by a controller; (ii) correct inaccuracies in their personal data; (iii) delete personal data provided by or obtained about the consumer; and (iv) obtain a copy of the personal data that the consumer previously provided to the controller in a portable and readily usable format;
- Requiring a formal appeal process for consumers if a controller refuses to take action on a consumer request; and
- Requiring written contracts between controllers and processors which set forth the instructions for processing personal data, the nature and purpose of processing, the duration of the processing, and the rights and obligations of both parties.
- Determining whether a person is acting as a "controller" or "processor" is a fact-based determination and each party's role should be defined within the contract.

## Broad Exemptions

The Act contains far broader exemptions than other state privacy laws. Specifically, it exempts "financial institutions or data subject to" the Gramm-Leach Bliley Act (GLBA). This is a significant shift from other laws like the CCPA whose exemption only applies to data subject to the GLBA. The Act also includes exemptions for covered entities and business associates under the Health Insurance Portability and Accountability Act (HIPAA), non-profits, and educational institutions.

## Enforcement

The Virginia Attorney General has exclusive authority to enforce the Act. Any controller or processor that violates the Act could face a penalty of up to \$7,500 for each violation. The Act does not contain a private right of action for consumers.

## Key Takeaways

The Act aggregates many terms, rights, and compliance obligations found in other privacy legislation like the GDPR, CCPA, and CPRA. While there are many similarities to the CCPA and CPRA, businesses that are subject to those laws cannot and should not assume that their prior compliance efforts in California or the EU are sufficient to comply with the Act. The Act contains several unique provisions that require action, including:

- Providing additional rights allowing consumers to opt out of the processing of personal data relating to targeted advertising
- Requiring businesses to perform a detailed analysis of processing activities between "controllers" and "processors" and to specifically outline the rights and responsibilities of each in written contracts

Virginia's Act is just the tip of the iceberg for new privacy legislation expected this year. At least 15 other states, [including New York](#), have either introduced new privacy legislation or have privacy bills in committee. Each state law will have varying terms and scopes, and will impose unique compliance obligations on covered businesses. Therefore, it is imperative for businesses to perform a comprehensive review of their privacy management programs, understand what personal information is collected from individuals, and how that personal information is being used by the business. Performing these tasks now will help ease the burden of addressing the litany of compliance obligations from these new laws.

If you have any questions regarding Virginia's Consumer Data Protection Act, other state privacy legislation, or any other aspect of your privacy management program, please contact the authors, [Alex Koskey](#) or [Matt White](#), or any member of [Baker Donelson's Data Protection, Privacy, and Cybersecurity Team](#).