Virginia Joining California With Adoption of Broad Data Privacy Protections: Controllers' Obligations Under Virginia's New Data Privacy Law

03.04.2021

Virginia is on the cusp of adopting of the **Consumer Data Protection Act** (CDPA). The bill passed the state Senate unanimously (39-0) and with significant support from the Virginia House (89-9). Governor Northam is expected to sign the Act shortly after the legislature adjourns on March 1, 2021. Virginia is the second state to adopt such privacy legislation after California lead the way with the **California Consumer Privacy Act** (CCPA), which took effect on January 1, 2020, and its recent passage of the **California Privacy Rights Act** (CPRA), which will take effect on January 1, 2023. A number of other states are likely to enact privacy acts in the coming year, including **Minnesota**, **New York**, **North Dakota**, **Oklahoma**, and **Washington** so keep your eye out for more updates.

The Governor of Virginia enjoys a line item veto, so the bill is subject to change but as currently formulated the CDPA provides the following:

Effective Date

- If signed by the Governor, the Act would become effective January 1, 2023.

Scope

- In its current form, the CDPA would apply to the following entities:
  - "persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth"; **and that**
  - (i) during a calendar year, control or process personal data of at least 100,000 consumers; **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."
- Unlike the California Act, the CDPA does not contain a revenue threshold.

Key Definitions

- The term "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 natural person acting in a commercial or employment context."
- The term "personal data" is defined broadly as "any information that is linked or reasonably linkable to an identified or identifiable natural person."
- The CDPA excludes "de-identified" and publicly available information under the definition. "De-identified" data is that which "cannot reasonably be linked to an identified or identifiable natural person or a device linked to such person."
- A "controller" means "the natural or legal person, that, alone or jointly with others, determines the purpose and means of processing personal data."
- A "processor" means a "natural or legal entity that processes personal data on behalf of a controller."

Responsibilities of Controllers and Processors

- The CDPA assigns certain obligations to data "controllers" and "processors."
- Controllers will be required to provide consumers with a privacy notice disclosing basic information such as the categories of personal data collected, the purpose for the collection, and how consumers can exercise their rights.
- Controllers must limit their data collection of personal data to that which is "reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer." The controller may not process personal data for purposes not reasonably necessary to, or compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, in the absence of express consent from the consumer.
- The CDPA also requires express consent from the consumer to process "sensitive data," defined as:
  - Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
  - The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;

  - The personal data collected from a known child; or
  - Precise geolocation data.
- Controllers are also required to implement reasonable security practices to protect to data.
- Processors must "adhere to the instructions of a controller" and assist them in complying with their obligations under the bill, pursuant to certain required terms of the **data processing agreement** with the controller, enumerated in the CDPA.
- Controllers are required to conduct a **data protection assessment** before engaging in data processing activities which involve:
  - Processing sensitive data;
  - Processing personal data for the purpose of targeted advertising;
  - Selling personal data;
  - Processing personal data for profiling purposes in certain contexts;
  - Processing personal data which presents a heightened risk of harm to consumers.

Statutory Exemptions

- The CDPA contains numerous exemptions. Non-profits and institutions of higher education are expressly exempt, as are organizations regulated by HIPAA as covered entities or business associates, and financial institutions or data subject to Title V of the federal Gramm-Leach-Bliley Act.
- The CDPA also exempts certain categories of data, primarily in situations where the data is already subject to federal regulation, such as HIPAA personal health information, personal data regulated by the Family Educational Rights & Privacy Act ("FERPA"), employment-related data, and certain types of data regulated by the Fair Credit Reporting Act ("FCRA").

Consumer Privacy Rights

- At present, the CDPA provides residents of the Commonwealth with the following rights:
  - confirm whether or not a controller is processing the consumer's personal data and to access such that data;
  - correct any inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;
  - delete personal data provided by or obtained about the consumer;

  - obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and
  - opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
- Controllers are required to respond to a consumer's request within 45 days.
- The term "sale of personal data" is defined as "the exchange of personal data for monetary consideration by the controller to a third party." Unlike the California Act, the CDPA's definition does not include the additional category of "other monetary consideration." as does the CCPA's definition of "sale."
- The CDPA also excludes the following disclosures from its definition of the "sale of personal data":
  - The disclosure of personal data to a processor that processes the personal data on behalf of the controller;
  - The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
  - The disclosure or transfer of personal data to an affiliate of the controller;
  - The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or
  - The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

Enforcement

The CDPA does not have a private right of action, meaning consumers are not permitted to directly sue a controller. Rather, the Virginia Attorney General's office is tasked with the exclusive authority to enforce the Act. The AG is required to provide 30 days' notice of any violation and allow the controller or processor to cure it. If the violation remains uncured, the office could file an action seeking up to $7,500 per violation.

Bailey Glasser stands ready to assist you if you have any questions regarding the CDPA. Visit us at www.baileyglasser.com or learn more about our firm here, or other Firm News & Insights, and on LinkedIn, Twitter, Facebook, Instagram, and YouTube.

This material is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or the Firm. **Michael Murphy**, a Bailey & Glasser partner licensed to practice law in the District of Columbia, New York, Washington, and West Virginia, **Jonathan Deem**, a Bailey & Glasser partner licensed to practice law in the District of Columbia, Virginia, and West Virginia, and **Elliott McGraw**, a Bailey & Glasser associate licensed to practice law in the District of Columbia, California, and New York, and Certified Information Privacy Professional, US (CIPP) contributed to the content of this material. The views expressed in this material are the views of the authors except as otherwise noted.

Attorneys

Jonathan S. Deem

Elliott McGraw

Michael L. Murphy