FAQs: Virginia Consumer Data Protection Act

By: Kevin D. Pomfret

03.10.2021

Virginia Governor Ralph Northam signed the Consumer Data Protection Act (the ?Act?) on March 2, 2021. The following are answers to some frequently asked questions about the Act and its impact on organizations doing business in Virginia.

When Does the Act Take Effect?

The Act takes effect on January 1, 2023.

Who is Protected by the Act?

The Act protects residents of Virginia when they are acting as consumers (in an individual or household context). It does not apply when they are acting as employees.

What Information Does the Act Protect?

The Act protects personal data, which is defined as ?any information that is linked or reasonably linkable to an identified or identifiable natural person.? Personal data that have been deidentified or made pseudonymous are excluded from the definition.

What Organizations Are Subject to the Act?

The Act generally applies to for-profit organizations that conduct business in Virginia or produce products or services that are targeted to residents of Virginia that:

- During a calendar year, control or process personal data of at least 100,000 consumers; or
- Control or process personal data of at least 25,000 consumers and derive over fifty (50) percent of their gross revenue from the sale of personal data.

Are Any Organizations Exempt from the Act?

A number of organizations are exempt from the Act, including:

- Commonwealth of Virginia bodies, authorities, bureaus, commissions, districts or agencies andany political subdivisions;
- Financial institutions subject to the Gramm-Leach-Bliley Act;
- Covered entities or business associates subject to the Health Insurance Portability and Accountability Act (HIPAA);
- Nonprofit organizations; and
- Institutions of higher education.

Are Any Types of Personal Data Exempt From the Act?

There are many types of personal data that are fully or partially exempt from the Act?s provisions, including:

- Personal data that are already otherwise subject to regulation, such as:
    - Protected health information under HIPAA;
    - Personal information regulated by the Fair Credit Reporting Act;
    - Personal data regulated by the Driver's Privacy Protection Act of 1994;
    - Personal data regulated by the Family Educational Rights and Privacy; and
    - Personal data subject to the Farm Credit Act.
- Personal data collected in the course of an individual applying to, employed by, or acting as an agent or independent contractor, provided that the data are collected and used for that purpose, and related data:
    - Collected as emergency contact information used for emergency contact purposes; or
    - That are necessary to retain and used to administer benefits.

What Rights Do Virginia Residents Have Under the Act?

The Act gives Virginia residents several important rights with respect to their personal data, including the rights to request that a controller:

- Confirm whether it is processing the consumer's personal data and, if so, to access such personal data;
- Provide 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 - where the processing is carried out by automated means

- Delete personal data provided by or obtained about the consumer;
- Correct inaccuracies in the consumer's personal data (taking into account the nature of the personal data and the purposes of the processing);
- Allow the consumer to 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.

When Is My Organization Considered a Controller?

A controller is defined as an organization that ?alone or jointly with others, determines the purpose and means of processing personal data.? Generally, this is the organization that collects the personal information.

What is Processing?

Processing is defined as ?any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data.?

What Are My Organization?s Responsibilities as a Controller?

If an organization is subject to the Act, its duties as a controller include:

- Limiting the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data are processed and as disclosed to the consumer;
- With certain exceptions, not process personal data for purposes that are neither reasonably necessary to nor compatible with the purposes for which the personal data are processed and as disclosed to the consumer, unless the consumer's consent has been obtained;
- Establishing, implementing, and maintaining reasonable administrative, technical, and physical data security practices ? appropriate to the volume and nature of the personal data;
- Not processing personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers;
- Ensuring that agreements with processors are compliant with the Act;
- Respond to the consumer requests regarding their personal data within 45 days. (In some instances, the response period may be extended by 45 additional days.); and
- Establish a process for a consumer to appeal a refusal to take action on a consumer request.

What Should Be Included in an Agreement Between a Controller and a Processor?

An agreement between a controller and a processor should include:

- The nature and purpose of processing;
- The type of data subject to processing;
- The duration of processing; and
- The rights and obligations of both parties.

The agreement should also include requirements that the processor:

- Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
- Delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;
- Upon reasonable request, make available all information in its possession necessary to demonstrate the processor's compliance with its obligations;
- Allow, and cooperate with, reasonable assessments by the controller of the processor's policies and technical/organizational measures; and
- Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations with respect to the personal data.

When Can a Consumer Opt-Out of Processing?

A consumer may opt out of the processing of personal data for:

- Targeted advertising;
- The sale of personal data, or
- Profiling for decisions that have a legal or similarly significant effect on the consumer.

What Constitutes the Sale of Personal Data?

The sale of personal data is defined as the exchange of personal data for monetary consideration. However, the following transactions are specifically excluded from the definition:

- 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 intentionally made available to the general public (i.e. through social media) and that was not restricted to a specific audience; or
- The disclosure or transfer of personal data to a third party as part of a merger, acquisition,

bankruptcy or similar transaction.

What Are Sensitive Data?

Sensitive data are defined as personal data:

- Revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation or citizenship or immigration status;
- Genetic or biometric data processed for the purpose of uniquely identifying a natural person;
- Collected from a known child under the age of 13; or
- Precise geolocation data.

What Is My Organization?s Responsibility Regarding Sensitive Data?

The Act states that a controller may not process sensitive data without the consumer?s consent (i.e. opt-in and preparation of a Data Processing Assessment.

What Is a Data Processing Assessment (DPA)?

A DPA is a document that (i) identifies and weighs the benefits of processing to the controller, the consumer, other stakeholders and the public against the potential risks to the affected consumer, and (ii) puts safeguards in place to mitigate such risks.

When Must an Organization Prepare A DPA?

An organization should prepare a DPA if it conducts the following activities:

- Processing personal data for purposes of targeted advertising;
- The sale of personal data;
- Processing personal data for profiling, where such profiling presents a reasonably foreseeable risk of:
- Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- Financial, physical, or reputational injury to consumers;
- Physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns of consumers, where such intrusion would be offensive to a reasonable person; or
- Other substantial injury to consumers;
- Processing of sensitive data; or
- Any processing of personal data that presents a heightened risk of harm to consumers.

What Elements Should Be Included in a Privacy Notice?

A privacy notice should include the following:

- The categories of personal data processed by the controller;
- The purpose for processing personal data;
- How consumers may exercise their rights;
- The categories of personal data that the controller shares with third parties, if any; and
- The categories of third parties, if any, with whom the controller shares personal data.

In addition, if an organization sells personal data or processes personal data for targeted advertising, the privacy notice should disclose such processing, as well as how a consumer may opt out.

When Should My Organization Begin the Process to Become Compliant by January 1, 2023?

If your organization is already compliant with the General Data Protection Regulation (GDPR) or with California?s Consumer Privacy Act (CCPA), then it likely does not need to begin right away. (However, it would be prudent to understand whether the differences between those two laws and the Act impact your organization, such as how sensitive information is treated.) If your organization does not currently comply with either the GDPR or the CCPA and you believe it might be subject to the Act by 2023, it should begin mapping your organization?s data supply chain (i.e. inbound collection/internal use/outbound transfers) as soon as possible, as the process of becoming compliant may take many months.

What Are the Penalties for Failing to Comply with the Act?

The Act does not provide for a private cause of action. Virginia?s Attorney General can impose a civil penalty of not more than $7500 for each violation.

Related People

- Kevin D. Pomfret ? 703.760.5204 ? kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity