whitepaper

VIRGINIA CONSUMER DATA PROTECTION ACT

The CDPA will be enforced by the Virginia Office of the Attorney General and the office may seek injunctive relief or civil penalties in the event of non-compliance.

On March 2, 2021, Governor Ralph Northam signed the Virginia Consumer Data Protection Act (CDPA)[1] into law.

The Act is substantively similar to recent privacy legislation enacted in California with some small differences. The CDPA will be enforced by the Virginia Office of the Attorney General and the office may seek injunctive relief or civil penalties in the event of non-compliance.

The CDPA will not become effective until January 1, 2023. The CDPA notably provides the same federal Fair Credit Reporting Act (FCRA) exemption set forth under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), excluding personal information used by a consumer reporting agency to generate a consumer report under the FCRA.

APPLICABILITY

The CDPA applies to entities that conduct business in the commonwealth and either:

- Control or process personal data of at least 100,000 consumers; or
- Derive more than 50% of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers[2].

Unlike the CCPA, the requirements do not apply to entities that generate a certain amount of revenue. Additionally, the CDPA broadly defines "personal data" to include any information that is linked or reasonably linkable to an identified or identifiable natural person.[3] A "consumer" includes any natural person who is a resident of the Commonwealth and acts only in "an individual or household context"; this does not include a natural person acting in a commercial or employment context.[4]

EXEMPTIONS[5]

The law provides for two different categories of exemptions: *entity level* and *data level* exemptions.

Entity Level Exemptions

There are five different entities that are exempt from compliance under the Act. These entities include:

- A body, authority, board, bureau, commission, district, or Virginian agency or any Virginian political subdivision.
- Any financial institution or data subject to the Gramm-Leach-Bliley Act (GLBA).
- A covered entity or business subject to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act.
- A nonprofit organization.

1 Va. Code. Ann. Section 59.1-571 through 59.1-581 Consumer Data Protection Act ("CDPA").
2 CDPA § 59.1-572
3 CDPA § 59.1-571
4 *Id.*
5 CDPA § 59.1-572

- An institution of higher education.

Data Level Exemptions:

There are fourteen different categories of data that are excluded from the CDPA. The most notable exemption is the Fair Credit Reporting Act exemption under § 59.1-572 C (10) which covers "the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.)."

In addition to consumer reporting, the Act will not apply to specific employee and job applicant data, as well as datasets regulated by:

- GLBA
- Drivers Privacy Protection Act
- Farm Credit Act
- Family Educational Rights and Privacy Act.

CONSUMER RIGHTS

The CDPA provides rights[6] that are similar to those provided under the GDPR and the CCPA. Unlike the CCPA and the CPRA, the CDPA does not prescribe how consumers must submit requests to exercise their rights.[7] These rights include:

1. Right to be informed

All consumers have the right to be informed of the data a business is collecting and processing. This right also allows the consumer to access such personal data.

2. Right to correct

The CDPA allows consumers the right to correct any inaccuracies in their respective personal data. The right to correct must take into account the nature of the data and the purposes for processing.

3. Right to data deletion

Consumers are able to delete any information provided by or obtained about the consumer.

4. Right to data portability

This right allows consumers to obtain a copy of the personal data that was previously provided to the controller in a portable and readily usable format. The consumer must be able to transmit the data to another controller through automatic means.

5. Right to opt out

Consumers have the right to opt out of having their data processed for the 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.

6. Right to appeal

In the event a business refuses to act within a reasonable time, a consumer has the right to appeal such decision. Businesses are required to respond to requests within 45 days and may extend this time window by an additional 45 days only if (1) reasonably necessary and (2) the business notifies the consumer. Controllers are required to establish an appeal process for consumers.

BUSINESS OBLIGATIONS

The CDPA differentiates between controllers and processors. A *controller* is a company that is responsible for determining the purpose and means of processing while a *processor* is a company that processes personal data on the controller's behalf.[8] "Processing" refers to any operation performed on personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.[9] This distinction is similar to the GDPR.

6 CDPA § 59.1-573

7 When implementing means to allow consumers to exercise their rights, Controllers must consider (1) the ways in which a consumer normally interacts with the controller; (2) the need for secure and reliable communication; and (3) the ability of the controller to authenticate the identity of the consumer making the request. The CDPA does not specify any specific manner that must be used.

8 CDPA § 59.1-571

9 *Id.*

The CDPA creates several obligations[10] for entities that are considered **controllers**. These obligations include:

- ***Consent for Sensitive Data***
  Controllers must obtain a consumer's consent before processing any sensitive data. Sensitive data might include information pertaining to an individual's location, genetic or biometric information, or physical/mental health. Additionally, the specific purpose for processing must be made clear to the consumer to ensure valid consent.

- ***Limited Collection and Use***
  Controllers must limit the collection of personal data to what is adequate, relevant, and reasonably necessary for the states purpose. If a controller processes data in a manner that is not compatible to the disclosed purpose, the controller must obtain additional consent from the consumer.

- ***Technological Safeguards with "Reasonable Security"***
  Controllers must establish, implement, and maintain reasonable technical and physical security practices. Controllers must further ensure that confidential information is protected and can only be accessed by authorized personnel.

- ***Privacy Policy and Data Protection Assessment***
  Consumers must be provided with a clear and meaningful privacy notice that includes: (i) the categories of personal data processed by the controller; (ii) the purpose for processing personal data; (iii) how consumers may exercise their consumer rights, which includes the right to appeal; (iv) the categories of personal data that the controller shares with third parties; and (v) the categories of third parties that might receive information.[11]
  The Data Protection Assessment is an additional obligation that requires the controller to assess processing activities that involve personal data. These activities include: (1) processing data for targeted advertising; (2) sale of personal data; (3) processing of data for profiling purposes; (4) processing sensitive data; (5) processing of personal data that presents a heightened risk of harm.[12] This assessment shall identify the risks of processing such information and weigh those against the available benefits. Controllers are expected to focus on the potential risks to the rights of consumers and ensure that the consumer is protected.

CONCLUSION

The Consumer Data Protection Act (CDPA) is now the second privacy legislation enacted in the United States. The CDPA is similar to obligations set forth under the CCPA and the CPRA; however, the CDPA does have some key differences. These differences include the controller/processor distinction as well as the broad requirements for notifying consumers of their rights. Additionally, the CDPA exempts personal information that is collected, maintained, disclosed, or sold by a consumer reporting agency who provides such information for use in a consumer report as defined by the FCRA.

Organizations that conduct background screening are well advised to consult with legal counsel before determining whether their use of consumer reports is exempt from the CDPA.

10 CDPA § 59.1-574
11 CDPA § 59.1-574(C)
12 CDPA § 59.1-576