Cybersecurity, Privacy and Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Virginia Consumer Data Protection Act: What Businesses Need to Know

March 4, 2021

On March 2, 2021, the Governor of Virginia signed the Virginia Consumer Data Protection Act (CDPA) into law, which goes into effect on January 1, 2023. The law applies only to businesses with large amounts of consumer data and does not apply to employee or business-to-business (B2B) data. The CDPA also provides broad exemptions, including for financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) and covered entities and business associates subject to the Health Insurance Portability and Accountability Act (HIPAA). Broad in scope, the CDPA incorporates aspects of the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), and the EU General Data Protection Regulation (GDPR).

Below, we have outlined some key aspects of the CDPA and have compared it to these other comprehensive privacy laws.

Who Must Comply with the CDPA?

Businesses are subject to the CDPA if **both** of the following criteria are met:

- They either conduct business in Virginia or produce products or services that are targeted to Virginia residents, and
- During a calendar year (i) 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 their gross revenue from the sale of personal data.

The Virginia law does not have a revenue threshold, and thus many large businesses that do not hold a substantial amount of consumer data will **not** be subject to the law. As noted below, the law explicitly excludes B2B and employee data from the definition of consumer, noting that "consumer" does not include individuals "acting in a commercial or employment context."

Which Entities—and What Data—Is Exempt?

The CDPA does not apply to certain government agencies, financial institutions subject to the GBLA, covered entities or business associates governed by HIPAA, nonprofit organizations and institutions of higher education. The CDPA also exempts certain data, including data protected by federal laws like HIPAA, the GLBA, the Fair

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Molly E. Whitman
Counsel
mwhitman@akingump.com
Los Angeles
+1 310.728.3737

Lauren E. York
Counsel
lyork@akingump.com
Dallas
+1 214.969.4395

Rachel Claire Kurzweil
Associate
rkurzweil@akingump.com
Washington, D.C.
+1 202.887.4253

Tina M. Jeffcoat
Associate
cjeffcoat@akingump.com
Dallas
+1 214.969.2741

Credit Reporting Act, the Driver's License Protection Act and the Family Educational Rights and Privacy Act. The CDPA further exempts data processed or maintained: (i) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role; (ii) as emergency contact information for an individual; or (iii) that is necessary to retain to administer benefits for another individual. Additionally, controllers and processors that comply with verifiable parent consent requirements under the Children's Online Privacy Protection Act shall be deemed compliant with any parental consent obligations under the CDPA.

What is "Personal Data" Under the CDPA?

As with other comprehensive privacy laws, the CDPA defines "personal data" broadly as "any information that is linked or reasonably linkable to an identified or identifiable natural person." Notably, the CDPA does not aim to capture Virginia residents in the employment and B2B context as the CCPA does. Instead, under the CDPA a "consumer" is defined as a natural person who is a resident of the Commonwealth "acting only in an individual or household context" and "does not include a natural person acting in a commercial or employment context."

Similar to the GDPR and the CPRA, the CDPA regulates "sensitive data." Sensitive data is defined as a category of personal data that includes: (i) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation or citizenship or immigration status; (ii) genetic or biometric data for the purpose of uniquely identifying a natural person; (iii) personal data collected from a known child; or (iv) precise geolocation data. The protections for sensitive data are discussed further below.

How Does The CDPA Apply Differently to Controllers and Processors?

Like the GDPR, the CDPA differentiates between controllers (companies that are responsible for determining the purpose and means of processing personal data) and processors (companies that process personal data on controllers' behalf). Under the CDPA, businesses who constitute "controllers" have more stringent obligations. In contrast, processors' obligations are generally connected to their contracts with controllers. For instance, processors are required to follow controllers' instructions; implement appropriate technical and organizational measures to help the controller respond to consumer rights; and provide the necessary information for controllers to comply with their data protection assessment obligations. Similar to the GDPR, the relationship between the controller and processor must be governed by a contract that includes certain specified requirements and obligations for the processor.

Obligations for Controllers

The CDPA places several responsibilities on controllers including:

- ***Limits on Collection and Use of Data***. The CDPA requires that controllers limit the collection of personal data to what is adequate, relevant and reasonably necessary for the purpose for which the data is processed. Controllers may not process personal data for purposes that are neither reasonably necessary for nor compatible with the disclosed purpose for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer consent.

- ***Reasonable Security***. Controllers must also establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such protections should be appropriate to the volume and nature of the personal data at issue.
- ***Consent for Processing Sensitive Data***. Controllers are required to obtain the consumer's consent before processing any sensitive data. Consent is defined similarly to the GDPR and the CPRA as a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to process personal data relating to the consumer and may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.
- ***Data Processing Agreements (DPAs)***. As noted above, the CDPA requires that controllers enter into DPAs with their data processors. These agreements must "clearly set forth instructions for processing data, 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 CDPA provides specific terms that must be included in any DPA.
- ***Privacy Notice***. Controllers must provide consumers with a reasonably accessible, 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, including how a consumer may appeal a controller's decision with regard to the consumer's request; (iv) the categories of personal data that the controller shares with third parties, if any; and (v) the categories of third parties, if any, with whom the controller shares personal data. This is similar to requirements for privacy policies under the CCPA and, to a more limited extent, under the GDPR.
- ***Notice of Sale***. Controllers that sell personal data to third parties or process personal data for targeted advertising must clearly and conspicuously disclose such processing in its privacy notice and provide a manner in which a consumer may exercise his or her opt out right. Unlike the CCPA, the CDPA does not appear to specify the specific manner in which the controller must prove the opt out right (i.e., there is no requirement for a specific link or button).
- ***Consumer Request Process***. Controllers must establish one or more secure means for consumers to submit requests to exercise their rights. Unlike the CCPA and CPRA, the CDPA is not prescriptive in how consumers must submit such requests, but provides that such means must take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request.
- ***Data Protection Assessment***. Controllers must conduct and document a data protection assessment for certain processing activities, including the sale of personal data, the processing of personal data for purposes of targeted advertising or profiling, the processing of sensitive data and any processing activities involving personal data that present a heightened risk of harm to consumers. These data protection assessments must identify and weigh the benefits to the business of processing consumers' data against potential risks to consumers associated with such processing. In balancing those competing concerns, businesses should consider whether certain safeguards, such as using de-identified data, would

mitigate risks to consumers, as well as consumers' reasonable expectations and the relationship between the business and the consumer.

What Rights Do Individuals Have Under the CDPA?

Similar to the CPRA and the GDPR, consumers have the following rights under the CDPA:

- ***Right to access***. Consumers have the right to confirm whether a controller is processing the consumer's personal data and obtain access to such data.
- ***Right to correct***. Consumers have the right to correct inaccuracies in the consumer's personal data.
- ***Right to delete***. Consumers have the right to delete personal data provided by or obtained about the consumer.
- ***Right to data portability***. Consumers have the right to obtain a copy of the consumer's personal data in a portable and readily usable format.
- ***Right to opt out of certain data processing***. Consumers will have the right to opt out of the processing of personal data for purposes of: (i) targeted advertising; (ii) the sale of personal data; or (iii) profiling in further of decisions that produce legal or similarly significant effects concerning the consumer. A "sale" under the CDPA is defined more narrowly than under the CCPA or CPRA to mean the exchange of personal data for **monetary** consideration by the controller to a third party.

The CDPA does not provide for any hardship exemptions to these rights. Businesses must respond to requests within 45 days of receipt of the request and may extend where reasonably necessary for an additional 45 days if the consumer is notified within the first 45-day window. Businesses must establish procedures for consumers to appeal a failure to act on a rights request within a reasonable time period and inform consumers of how they can submit a complaint to the attorney general if the appeal is denied.

Who Enforces the CDPA?

The Virginia Attorney General has exclusive authority to enforce the CDPA and to impose a civil penalty of up to $7,500 per violation. Businesses may avoid an enforcement action, however, by properly remedying the violation. The CDPA's right to cure allows businesses to correct any violation of the CDPA within 30 days of receiving notice thereof from the Virginia Attorney General. Unlike the CCPA, the CDPA does **not** provide a private right of action to consumers.

The CDPA also requires businesses to establish procedures for consumers to appeal any denial of their rights under the CDPA. This appeal right, coupled with the provision for enforcement by the attorney general and the possibility of hefty civil fines, may compensate for the lack of a private right of action in the CDPA.

Key Takeaways

Businesses subject to the CDPA will need to perform a comprehensive data inventory and update their external policies and internal procedures to come into compliance. The CDPA requires businesses to conduct data protection assessments for specified processing activities and to establish procedures by which consumers may appeal any denial of their CDPA rights. Businesses must also update their public-facing privacy

policies to, among other changes, make a public commitment to not re-identify de-identified personal data and provide details on its data processing activities. The CDPA extends its protections to businesses' contracts with service providers by requiring businesses to limit the service provider's use and further distribution of personal data. Notably, the CDPA does not displace or change businesses' existing obligations to report data breaches.

Looking Ahead

The CDPA's quick pace toward enactment may foreshadow its role as a blueprint for other states looking to enact comprehensive data privacy reform. The CDPA was designed to provide key protections for consumers and clearly define the obligations for businesses to ensure a smooth path toward compliance, without imposing overly burdensome requirements in a complicated statutory structure. As State Sen. David Marsden, who introduced the legislation, described, "This is a huge step forward. By creating this omnibus bill, we take the lead in data privacy in the United States. This omnibus bill is clear, concise, and holds companies accountable for protecting consumer data in providing protections for consumers."

On the federal level, it has already been predicted that the Biden administration will be active in the federal data privacy movement, given the Obama administration's steps toward a federal privacy regulatory framework and Vice President Kamala Harris's support for data privacy initiatives during her time as California's attorney general. With several other states poised to follow Virginia with their own comprehensive privacy legislation, Congress may shift its priorities in the direction of a federal standard.

akingump.com