March 10, 2021

Skadden

Privacy & Cybersecurity

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Gabriella Manduca
Law Clerk / New York
212.735.3202
gabriella.manduca@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

Virginia Becomes Second State To Adopt Comprehensive Privacy Law

On March 2, 2021, Virginia Gov. Ralph Northam signed into law the Virginia Consumer Data Protection Act (CDPA), making Virginia the second state after California to enact comprehensive privacy legislation. The CDPA will become effective on January 1, 2023, the same day the California Privacy Rights Act (CPRA) comes into effect, replacing the current California Consumer Privacy Act (CCPA), which went into effect in 2020.

The new Virginia law draws on concepts from the European Union's General Data Protection Regulation (GDPR) (such as the use of "controllers" and "processors") and from California's laws (such as the rights of consumers). The net result will be a more complicated privacy compliance environment for companies that will be further exacerbated if additional states enact their own "similar but different" approaches to privacy law.

Which Businesses Are Covered?

The CDPA applies to entities that conduct business in Virginia and those that conduct business outside of Virginia but offer products or services to Virginia residents if they:

- control or process the personal data of at least 100,000 consumers during a calendar year, or
- control or process the personal data of at least 25,000 consumers and derive at least 50% of their gross revenue from the sale of personal data.

Importantly, in contrast to California, which applies to any company with more than $25 million in revenue (regardless of how much personal data it processes), Virginia's law does not include a revenue trigger. Thus, large entities will not be subject to the CDPA if they do not meet the personal data thresholds above.

Another important contrast to the CCPA/CPRA is that the Virginia law explicitly carves out personal data of employees or business-to-business data. While California law has adopted a temporary carve-out for those categories of data, that carve-out is slated to end on January 1, 2023.

The Virginia law includes certain important carve-outs. For example, it does not apply to entities subject to the federal Gramm-Leach-Bliley Act governing financial institutions, or the Health Insurance Portability and Accountability Act (HIPAA), even if the personal data at issue is not itself covered by those laws. Note that under the CCPA, only personal data that was subject to those laws was carved out. Other exempt entities include governmental

entities, nonprofit organizations and higher education institutions. The CDPA also exempts specific information regulated by certain federal laws, such as the Children's Online Privacy Protection Act and the Driver's Privacy Protection Act.

Which Consumers Are Covered?

A "consumer" under the CDPA is "a natural person who is a resident of the Commonwealth [of Virginia] acting only in an individual or household context."

Definition of Personal Data

"Personal data" under the CDPA is "any information that is linked or reasonably linkable to an identified or identifiable natural person." The Virginia law thus adopts the broad definition of personal data that has become increasingly commonplace: namely, data that itself might not identify an individual is still personal data if it can be "reasonably linkable" to an individual. In contrast to the California laws, the CDPA does not include information linkable to "households," a concept that has raised many questions of interpretation under the CCPA.

Personal data does not, however, include de-identified data or publicly available information. Like the CCPA in California, the CDPA defines "publicly available information" to include information lawfully made available through government records. Significantly, the CDPA also excludes information that a business "has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information unless the consumer has restricted the information to a specific audience." While the manner in which this clause will be interpreted remains to be seen, it provides businesses with the opportunity to determine that certain information is not personal data because the data subject has publicly posted such information on social media.

"Pseudonymous data" (*i.e.*, "personal data that cannot be attributed to a specific natural person without the use of additional information") is exempt from consumer rights requests if it is "kept separately and is subject to effective [documented] technical and organizational controls that prevent the controller from accessing such information." The CDPA also adds an administrative burden by requiring data controllers that disclose pseudonymous data to exercise reasonable oversight to "monitor compliance with any contractual commitments" to which the pseudonymous data is subject, and to take appropriate steps to address any breaches of such commitments.

Controllers and Processors

Like the GDPR, the CDPA creates categories of "controllers" and "processors" with differing obligations. A controller is the entity that determines the purpose and means of processing personal data, whereas a processor processes personal data on the controller's behalf.

Consumer Rights

As with the CCPA, the CDPA grants consumers a series of privacy rights, using similar time periods to the CCPA. Specifically, a consumer may exercise the following rights up to twice a year, and entities must respond within 45 days, with one 45-day extension, provided the consumer is so notified within the initial period. However, in contrast to the CCPA, which provides certain limitations on a consumer's rights, the CDPA is broadly and simply stated with no enumerated exceptions. In addition, the CDPA does not include the CCPA's concept of allowing "authorized agents" to exercise rights on behalf of a consumer, thus omitting a concept that is likely to create a compliance burden under California.

Rights of Access

Consumers have the right to confirm whether a controller is "processing the consumer's personal data and to access such personal data."

Right To Correct

Consumers have the right to require the controller to correct any inaccuracies in their personal data, taking into account the nature of the personal data and the purposes for which the personal data is being processed.

Right of Deletion

Consumers have the right to require that their data be deleted by the data controller. In contrast to the CCPA, which sets forth certain exceptions to the right of deletion, the CDPA offers no such exceptions. In addition, the right of deletion covers personal data provided by "or obtained about" the consumer, ostensibly from a third-party source. By contrast, the CCPA right of deletion only covers data the business has collected from the consumer.

Right of Portability

On request from a consumer, a controller must furnish a copy of the consumer's personal data in a portable and reasonably readily usable format that permits the consumer to transmit it to another controller.

Right To Opt Out

Like the CCPA, the CDPA creates a right to opt out of the sale of personal data, but it also includes a right to opt out of the processing of personal data for purposes of targeted advertising and "profiling that produce legal or similarly significant effects." A "sale of personal data" is deemed to occur when a third party gives a controller monetary consideration in exchange for personal data. This definition is narrower than the CCPA, which defines a sale as cases where personal data is provided in exchange for "monetary or other valuable consideration." Sales do not include disclosures to a third party as an asset transfer that is part of a merger, acquisition or other transaction in which the third party assumes control of the controller's assets.

Right To Appeal

The CDPA imposes an additional burden on companies that does not exist under the CCPA. A consumer has the right, "within a reasonable period of time," to appeal a decision by a controller to deny the exercise of one of the customer rights set forth above. The controller must establish an appeals process and act on a consumer's appeal within 60 days. If the appeal is denied, the controller must provide the consumer with a means to refer his or her concerns to the Virginia attorney general. The appeals process, which may require bespoke responses, could create an administrative burden for companies that process material amounts of personal data.

Sensitive Data

The CDPA requires entities to obtain opt-in consent to collect or process "sensitive data," which is defined as personal data relating to information about racial or ethnic origin, religion, health diagnosis, sexual orientation, citizenship or immigration status, biometric data, precise geolocation data or data collected from a person known to be under 13 years old. This is different from the CPRA, which only requires the provision of an opt-out mechanism (unless the data subject is a child). However, the definition of sensitive data under the CDPA is narrower than California's because it does not include items such as passport numbers and log-in credentials.

Obligations Imposed on Businesses

The CDPA imposes limits on the collection and use of personal information, as well as certain safeguards and transparency measures, as discussed below.

Limits on Collection and Use

The CDPA limits a controller to the collection of personal data that is "adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer." Data may not be processed for purposes that are not reasonably necessary nor compatible with the disclosed purposes for which the personal information is processed, as was disclosed to the consumer, without the consumer's prior consent. The "disclosure" requirement suggests that businesses will need to specify how they plan to use personal data before they do so.

Technical Safeguards and Transparency Measures

A controller must establish, implement and maintain reasonable administrative, technical and physical data security practices to protect personal data, commensurate to the volume and nature of the personal data at issue.

Data Protection Assessments

Controllers must conduct data protection assessments to evaluate the risks associated with a range of activities, including the sale of personal data, targeted advertising and profiling that presents a reasonably foreseeable risk of unfair or deceptive treatment, "an intrusion upon the solitude or seclusion, of privacy affairs or concerns, of consumers," the processing of sensitive personal data, and processing that leads to a "heightened risk of harm to consumers." Such an assessment is similar to the GDPR's data protection impact assessment requirement and must take into account privacy risks, benefits and potential mitigation steps in light of the specific use. Under the CDPA, entities may weigh the benefits incurred by processing the data against the risks the processing poses to the consumer.

Importantly, data protection impact assessments can be developed under attorney-client privilege. While the Virginia attorney general may obtain these assessments through a civil investigative demand, the attorney-client privilege is not deemed to be waived. Data protection assessments are also deemed confidential and exempt from public inspection under the Virginia Freedom of Information Act.

Data Processing Agreements and the Role of the Data Processor

Among the more onerous requirements imposed by the CDPA is that any processing activities undertaken by a third party on behalf of a controller must be governed by a data processing agreement setting forth such specifics as the instructions for processing, the nature and purpose of processing and the type of data being processed.

Data Processors

Data processors are obligated to adhere to the instructions of a controller and to assist the controller in meeting its obligations under the CDPA. They must also allow, and cooperate with, reasonable assessments (*i.e.*, an audit) by the controller or the controller's designated assessor, or arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures "using an appropriate and accepted control standard or framework and assessment procedure for such assessments." The processor is required to provide a report of such assessment to the controller upon request.

Privacy Policies

The CDPA requires controllers to provide consumers with a privacy policy, which must state the categories of personal data the controller processes, the purpose for processing personal data, the categories of personal data the controller shares with third parties, the categories of third parties with whom it shares personal data, and the means by which consumers can exercise their consumer rights and appeal a controller's decision regarding the consumer's request.

Enforcement

There is no private right of action for consumers under the CDPA; the Virginia attorney general has exclusive authority to enforce it. Once the attorney general decides to act, the office must notify the controller or processor, which then has 30 days to cure the violation and provide the attorney general with assurances that the alleged violations are cured and will not recur. If the controller or processor fails to cure, the attorney general may levy fines of up to $7,500 per violation. The cure period and the magnitude of the fines is commensurate with those in California.

Key Takeaways

Unlike the California law, the new Virginia law does not provide for a period of rulemaking by the attorney general. Thus, the ongoing revisions that have complicated the roll-out of the CCPA in California should not apply to the CDPA.

While the rights and obligations created by the CDPA echo those created by the CCPA, CPRA and, in some respects, the GDPR, businesses should not assume that compliance with those laws automatically translates into compliance with the CDPA. Moreover, while companies have almost two years to come into compliance with the CDPA, the enactment of this Virginia law, and the progress of privacy laws in other state legislatures, means that companies will not be able to treat personal data of California residents as its own unique category.

Rather, companies should consider adopting comprehensive approaches to privacy using a "lowest common denominator" approach to make sure their programs comply with the laws of all applicable states. It remains to be seen whether the adoption of additional state laws creates pressure for a federal privacy law to ease the compliance burden on companies.