D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

MARCH 2021

DIGITAL MEDIA, TECHNOLOGY & PRIVACY

>> ALERT

VIRGINIA BECOMES THE SECOND STATE TO PASS A COMPREHENSIVE PRIVACY LAW

After passing with relative ease through Virginia's House of Delegates and Senate, Governor Ralph Northam signed the Virginia Consumer Data Protection Act (CDPA) into law on March 2, 2021.

Virginia joins California as the only states in the nation to have passed comprehensive privacy legislation. Companies that are subject to the new law will have to comply beginning January 1, 2023, the date when the law goes into effect. Companies should note that this date coincides with the effective date of the new substantive obligations set forth in the California Privacy Rights Act (CPRA), the recently passed ballot initiative amending the California Consumer Privacy Act (CCPA), as discussed in our previous alert.

While the new Virginia law creates a hybrid model that borrows liberally from the CCPA and CPRA, as well as the EU's General Data Protection Regulation (GDPR), it also contains many unique elements that diverge from these counterparts.

THE BOTTOM LINE

>> While Virginia is now the second state with a comprehensive consumer privacy law, it certainly will not be the last.

>> With CCPA already in effect and the CDPA and CPRA both on the horizon, companies will need to begin planning now to update their privacy programs to ensure compliance with these conflicting standards.

DETAILS OF THE CDPA

The threshold question for companies to consider will be whether the new law applies to their specific organization. The CDPA will apply to persons that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that controls or processes personal data of at least:

>> 100,000 "consumers" during a calendar year; or

>> 25,000 "consumers" and derives over 50 percent of gross revenue from the "sale" of personal data.

Consumer

It's important to understand that "consumer" only includes Virginia residents that *are acting in an individual or household context and specifically excludes persons acting in a commercial or employment context*. Accordingly, businesses do not need to consider data collected from its employees or from business contacts as personal data under the CDPA.

Sale of Personal Data

Businesses will need to consider whether they "sell" personal data under the law. Unlike its California counterpart, the "sale" of personal data is narrowly defined as "the exchange of personal data for monetary consideration by the controller to a third party." In other words, monetary consideration must be paid to the business in order for a "sale" to occur. The CDPA also specifically excludes, among other things, disclosures to a business' affiliate from the definition of a "sale".

Personal Data

As with any privacy law, the definition of personal data is critical to assessing the scope of the law. The CDPA simply defines "personal data" as information that is linked or reasonably linkable

>> continues on next page

to an identified or identifiable natural person. It specifically excludes de-identified data and publicly available information. The definition does not reference information that is linkable to a household, as is the case in the CCPA/CPRA.

Sensitive Data

Like the CPRA, the CDPA defines "sensitive data" to include personal data that reveals racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, as well as genetic or biometric data used for the purpose of uniquely identifying a natural person, the personal data collected from a known child, and precise geolocation data. Notably, a business will need to obtain a consumer's consent before it can process sensitive data.

CONSUMER RIGHTS

The CDPA makes available certain core rights to consumers (similar to those found in the GDPR). In fact, the new law uses the terms "controller" and "processor" which are the same terms used under GDPR, although the definitions are not identical.

In particular, the CDPA gives Virginia consumers the right to:

- Confirm whether or not a controller is processing the consumer's personal data and to access such data;
- Correct inaccuracies in their personal data;
- Delete their personal data;
- Obtain a copy of personal data that the consumer provided to the controller in a portable and, to the extent technically feasible, readily usable format; and
- Opt-out of certain types of processing, including the sale of personal data, as well as the use of personal data for purposes of "targeted advertising."

DATA CONTROLLER RESPONSIBILITIES

Limitations on Processing

Similar to the GDPR processing principles, the CDPA incorporates certain limits on processing that generally apply to the controller of personal data, which include obligations to:

- Limit the collection of personal data to what is "adequate, relevant and reasonably necessary" in relation to the purpose for which the data was collected;
- Implement and maintain reasonable security practices to protect personal data;
- Restrict the use of personal data for new purposes that are incompatible with the purposes for which it was collected;
- Not discriminate against consumers for exercising their consumer rights; and
- Obtain consent before processing any sensitive data.

Privacy Policy

Controllers are required to provide consumers with a privacy policy that is reasonably accessible and includes:

- The categories of personal data processed by the controller;
- The purpose for processing personal data;
- How consumers can exercise their rights (and appeal a controller's decision with regard to the consumer's requests);
- The categories of personal data shared with third parties; and
- The categories of third parties with whom personal data is shared.

Transparency Regarding Sales and Targeted Advertising

If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose such processing as well as the manner in which a consumer can opt-out. Notably, there is no mandate as to how these disclosures must be made.

>> continues on next page

Data Processing Agreements

Similar to the GDPR, the CDPA requires a contract to govern a processor's data processing procedures performed on behalf of the controller. The contract will need to set forth the 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. Certain mandatory requirements must also be imposed on the processor, including requirements to make available all information to demonstrate the processor's compliance with the CDPA, submit to assessments conducted by the controller (or, alternatively, have an independent assessment conducted), and to flow down the processor's obligations on any subcontractors engaged by the processor.

Data Protection Assessments

The CDPA also requires the controller to conduct data protection assessments of the risks associated with certain enumerated processing activities, including the processing of personal data for targeted advertising, the sale of personal data, the processing of personal data for profiling (if such profiling presents certain risks of harm to consumers), the processing of sensitive data, and other processing that presents a heightened risk of harm to consumers. The law does not specify how often such assessments must be conducted.

ENFORCEMENT; NO PRIVATE RIGHT OF ACTION

Enforcement of the CDPA will be the responsibility of the state attorney general. There is no private right of action. Notably, the CDPA contains a 30-day notice period that allows a controller to cure violations that have been brought to its attention by the attorney general. This contrasts with the CPRA which will remove a similar cure period that is currently included in the CCPA. Violations that have not been cured within 30 days are subject to a fine of up to $7,500 per violation.

FOR MORE INFORMATION

Richard S. Eisert
Partner
212.468.4863
reisert@dglaw.com

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

Justin H. Lee
Associate
212.468.4894
jlee@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
212.468.4800
1675 Broadway, New York, NY 10019
www.dglaw.com