Virginia Enacts a Comprehensive Privacy Law—Similarities and Differences Among VCDPA, CCPA and GDPR

March 5, 2021

Virginia has just become the second U.S. state with a comprehensive privacy law, with Governor Ralph Northam's signing of the Virginia Consumer Data Protection Act ("VCDPA") on March 2, 2021. The VCDPA bears a strong resemblance to the California Consumer Privacy Act ("CCPA"). It also pulls U.S. law in the direction of its overseas cousin, the European Union's General Data Protection Regulation ("GDPR").

The VCDPA will take effect on January 1, 2023. That gives businesses almost two years to plan for compliance. Perhaps the biggest decision will be whether companies should adopt a "highest common denominator" approach — that is, voluntarily treating the data of all consumers regardless of location as if it were subject to all of these increasingly stringent privacy laws. With more laws like VCDPA seeming likely to be enacted elsewhere, could highest common denominator now be the most operationally sensible way to go?

What Businesses Are Covered by VCDPA?

The VCDPA applies to "persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, 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 gross revenue from the sale of personal data." Just as the CCPA does not define "doing business" in California, VCDPA does not define "conduct[ing] business" in Virginia. The prudent assumption is that the same sort of economic activity that triggers tax liability or personal jurisdiction in Virginia will also trigger VCDPA applicability.

These coverage provisions mean the VCDPA will cover substantially the same group as the CCPA: medium to large for-profit businesses that interact with the state's residents.

What Data Is Covered by VCDPA?

VCDPA follows the CCPA and GDPR in applying a broad definition of personal data, sweeping well beyond the traditional U.S. notion of data that expressly identifies a person. It defines personal data as "any information that is linked or reasonably linkable to an identified or identifiable natural person." It does not include data that has been de-identified or data that is publicly available

Persons acting in either a commercial or employment context are excluded from the VCDPA's definition of "consumer." In addition, the data "processed or maintained" by employees or independent contractors acting on behalf of a covered business is exempted, so long as the data is used within that employment context.

What Exemptions or Carve-Outs from the VCDPA Can Businesses Take Advantage Of?

The most notable exemption is for organizations subject to the Gramm-Leach-Bliley Act ("GLBA"). Financial institutions should take note; this is broader protection than under CCPA, which provides an exception for ***data*** subject to GLBA, but not across the board for ***entities*** subject to GLBA. Like the CCPA, the VCDPA exempts entities covered under the Health Insurance Portability and Accountability Act ("HIPAA").

There is also a safe harbor for third-party violations. Controllers and processors disclosing personal data to third-party controllers and processors will not be held liable for the third-party's violation, absent knowledge of that party's intent to commit a violation.

How Does the VCDPA Handle Data-Related Profiling and Discrimination Risks?

The VCDPA addresses profiling-related risks to which all businesses falling under the legislation's provisions should pay close attention. For example, the legislation explicitly forbids the processing of personal data in violation of state and federal anti-discrimination laws, and specifically lists profiling as a ground on which consumers can opt-out of data processing.

Akin to GDPR, but going beyond CCPA, controllers must also undertake "data protection assessments" that judge the benefits of data processing along with risks to the consumer. Notably, controllers must assess the processing of personal data used for profiling when there is a "reasonably foreseeable risk" that such profiling will lead to

discriminatory impact; economic, reputational or actual harm; and invasions of privacy. The VCDPA assessments could well be required for a substantial amount of targeted advertising and AI activities.

Businesses employing AI and other algorithmic targeting in service of advertising or operations should dedicate a renewed energy to considering how current and future technologies can steer clear of profiling or discriminatory behavior. Though already best practice generally, this sort of internal diligence will be even more important once the VCDPA takes effect, and should other states follow suit.

What Are Consumers' Key Rights under the VCDPA?

Under the VCDPA, consumers have the right to make various requests to companies holding their data — what have commonly come to be known as data subject access requests, or DSARS. (Say "dee-sars" if you want to sound like a privacy pro). Under VCDPA, consumers can ask a company to:

- Confirm if a controller is processing their personal data and receive access to that data;
- Correct inaccuracies in their personal data;
- Delete their personal data;
- Provide a copy of their personal data; and
- Opt them out of the processing of their personal data used for (a) targeted advertising, (b) sale, or (c) profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."

The inclusion of profiling as grounds for a consumer opt-out request is modeled on the GDPR, though the VCDPA goes a step further. There are no exceptions to the profiling provision under the Virginia law, whereas the GDPR allows automated, profiling-based decisions when necessary for a contract between the consumer and controller, when authorized by the government or when consented to by the consumer.

What Is a Data "Controller" and What Are Their Responsibilities?

The VCDPA applies to entities that "control or process" personal data. The roles and legal duties of "controller" (think data owner) and "processor" (think vendor to the data owner) of course are fundamental to GDPR; this is the first time they have found their way significantly into U.S. law.

The controller is defined as the person or entity that, alone or with others, "determines the purpose and means of processing personal data." The VCDPA places a clear "purpose" limitation on controllers relative to the CCPA, prominently restricting consumer data collection to the intended and disclosed purposes, absent consumer permission. Part of that disclosure process includes providing clear and accessible privacy notices.

Controllers cannot discriminate against consumers for any purpose, nor can controllers process sensitive data without obtaining consumer consent. For processing the sensitive data concerning a "known child," under the age of thirteen, the controller must obtain "verifiable parental consent" (15 U.S.C. § 6501(9) (1998)).

How Does the VCDPA Regulate "Processors"?

The processor is "a natural or legal entity that processes personal data on behalf of a controller." Like the EU's GDPR, the VCDPA requires controllers and processors to enter into contracts governing how consumer data is processed. Such a contract must ensure each processor is subject to a duty of confidentiality with respect to the covered data. While this provision represents another import from the GDPR, a requirement to continuously police vendors has become a commonplace obligation in U.S. privacy regulation. Data can be outsourced; privacy law obligations cannot.

Who Enforces the VCDPA?

The Virginia Attorney General has exclusive authority to bring an action against controllers or processors. After providing non-compliant controllers and processors written notice of their violations, and if the entities fail to cure within a 30-day period, the Attorney General may seek an injunction or a civil penalty of up to $7,500 for each violation. There is no private right of action.

This arrangement is in contrast to GDPR, which allows for both regulatory enforcement and private litigation. It is also in (partial) contrast to CCPA, which vests

enforcement of most data privacy aspects of the law exclusively with California government authorities, but allows private lawsuits for data breaches.

What Should Companies Do to Plan for Compliance with the VCDPA?

It would be prudent to think about the following:

- **Consider whether you are in scope at all**. Most national B2C enterprises probably touch Virginia consumers, given the size and prominence of the state. But for some companies, it may be possible to avoid VCDPA altogether if significant Virginia touchpoints are lacking.

- **If in scope—consider whether a Virginia-specific compliance plan makes sense, or whether to adopt a national or global approach**. GDPR and CCPA, and the prospect of more such laws coming down the pike, have already caused some to treat all consumer data as if subject to the most stringent privacy laws. This entails voluntarily accepting the burdens of laws that may or may not apply (*e.g.*, if you don't hold Californian or European data) in exchange for the operational simplicity of treating all data alike. VCDPA intensifies the need to consider this option. The alternative is to try and build data privacy policies and procedures that segregate data by its geographic origin.

- **Establish processes to comply with legal obligations to consumers**. Businesses will need to ensure they have the functionality to offer consumers the choice to opt-in to the processing of their sensitive information, and to complete appeals within the 60-day statutory limit.

- **Assess contractual relationships where third parties are handling your consumers' data, or where you are handling data for other companies**. In accord with the VCDPA's requirement that controllers and processors enter into contracts regarding the processing of data, businesses should evaluate their data sharing and contractual arrangements to make sure future agreements are VCDPA-compliant.

- **Begin considering the benefits and risks of data collection and uses**. Entities that will be subject to VCDPA should begin preparation for the "data protection assessments" as soon as practically possible. Businesses would be particularly wise to begin vetting their current and planned use of AI and of targeted advertising.

- **Start tracking what types of consumer data your business collects**. Companies seeking to bring their operations into compliance with the VCDPA should also

undertake a diligence and data mapping exercise to determine what sort of personal information is being collected, held and shared by the institution and processors. From there, companies can conduct a gap analysis and begin updating or developing policies, procedures and technical measures to comply with the VCDPA.

If you are already compliant with the CCPA requirements, you have a good head-start at being VCDPA-ready. Companies that invest early in compliance will likely see significant returns as more states push similar laws.

VCDPA—CCPA—GDPR Comparison Chart

	VCDPA	CCPA	GDPR
Who is covered?	A person doing business in Virginia that: • Controls or processes the data of at least 100,000 consumers per year; or • Controls or processes the personal data of at least 25,000 consumers with over 50 percent of revenue coming from such sales	A person doing business in California that: • Has annual gross revenues above $25M; • Utilizes the personal data of at least 50k consumers, households, or devices; or • Derives half or more of its revenue from sales of personal data each year	Entities that: • Have an "establishment" in the EEA or target or monitor consumers in the EEA from outside the EEA
What types of entities are covered?	• "Controllers" defined as person or entity that, alone or with others, "determines the purpose and means of processing personal data," and meeting the above criteria • "Processors" defined as "a natural or legal entity that processes personal data on behalf of a controller"	• Businesses meeting the above criteria • Service Providers	• "Controllers" defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" • "Processors" defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
What are the main coverage exemptions?	• Organizations subject to the GLBA • Organizations subject to HIPAA requirements • Data collected pursuant to HIPAA,	• Organizations subject to HIPAA • Data subject to GLBA or the California Financial Information Privacy Act	• No comparable exemptions

	VCDPA	CCPA	GDPR
	the Fair Credit Reporting Act; Drivers' Privacy Protection Act; Family Educational Rights and Privacy Act; and employment-related data • Data collected in compliance with the Children's Online Privacy Protection Act	• Data collected pursuant the Fair Credit Reporting Act or the Driver's Privacy Protection Act; and employment related data	
What are a covered party's key obligations?	• Provide notice and obtain consent at the start of a transaction; • Respond to consumer requests regarding personal data, including requests for copies of personal data or deletion of personal data • Establish appeals procedures for denial of consumer requests • Adhere to purpose limitations for collection of data	• Provide notice of data collection at the start of a transaction; • Respond to consumer requests regarding personal data, including requests for copies of personal data or deletion personal data • Adhere to purpose limitations for collection of data	• Ensure have a lawful basis for processing personal data • Provide mandatory transparency information • Respond to consumer (and other data subject) requests regarding personal data, including requests for copies of personal data or deletion of personal data • Adhere to purpose limitations for use of data
What are covered entities' responsibilities with respect to de-identified data?	• Companies with de-identified data must take "reasonable measures" to prevent re-identification, and must contract with entities to whom de-identified data is disclosed to ensure they follow VCDPA requirements	• None, but de-identified data is only carved out of the definition of "personal data" when businesses institute procedures to prevent re-identification	• No obligations in respect of truly anonymized data • "Pseudonymized" data remains "personal data"
What are consumers'	Consumers have the	Consumers have the	Consumers have the

	VCDPA	CCPA	GDPR
key rights?	right to: • Confirm if a controller is processing their personal data and have access to that data • Correct inaccuracies in their personal data • Request deletion of personal data • Obtain a copy of their personal data, to be provided in a portable format • Opt out of the processing of their personal data used for (a) targeted advertising, (b) sale or (c) profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer"	right to: • Access personal information, including the categories of information collected and what personal information has been sold • Opt-out of data processing • Request deletion of their personal data • Request a copy of personal data spanning the previous twelve months, to be provided in a portable format • Request deletion, subject to certain exceptions, like law enforcement necessity • Opt out of the sale of their data only	right to: • Receive information about what data is being collected and how it is being shared • Access the records of their data, to be provided in a portable format • Correct their data • Request deletion of their data • Restrict usage and processing of their data for targeted advertising and profiling purposes • Object to the purposes for which data is being processed in certain cases • Not be subject to automated decision making, subject to certain carve-outs
Can consumers opt-out of data sales?	• Yes	• Yes, for the sale of data only (and the CPRA adds a right for consumers to reject the sharing of data)	• No but data sales may require a standalone lawful basis distinct from that used to collect personal data and can be difficult to establish
Do consumers have a right to opt-in to processing of sensitive information?	• Yes	• No, but consumers can opt-out	• "Special Category" data is subject to additional, more stringent "lawful basis" requirements. Consent may frequently be required.
Do consumers have a right of appeal when	• Yes	• No	• All consumers can make complaints to the relevant data

	VCDPA	CCPA	GDPR
requests involving their data are denied?			protection authority
Are there any cross-border transfer restrictions?	• No	• No	• Yes
Do consumers have a right of action?	• No	• Yes (but only with respect to data breaches)	• Yes
Who enforces the law?	• Virginia Attorney General	• California Attorney General	• Data Protection Supervisory Authorities established by member states
What are the possible penalties?	• A maximum of $7,500 for each violation	• For private actions, $100 to $750 per violation, or actual damages, whichever figure is greater; for enforcement actions, a maximum of $2,500 per violation or $7,500 for an intentional violation	• A maximum of €20M or 4% of global annual turnover, whichever figure is greater

To subscribe to the Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK


Jeremy Feigelson
jfeigelson@debevoise.com


Avi Gesser
agesser@debevoise.com


Anna R. Gressel
argressel@debevoise.com


Alexandra P. Swain
apswain@debevoise.com


Javier Alvarez-Oviedo
jalvarez@debevoise.com


Scott M. Caravello (Law Clerk)
smcaravello@debevoise.com


Tricia Reville (Law Clerk)
pmreville@debevoise.com

LONDON


Christopher Garrett
cgarrett@debevoise.com


Robert Maddox
rmaddox@debevoise.com