MARCH 2021

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

Virginia's Foray Into Comprehensive Privacy Law

For what seemed like an eternity (okay, just a couple years), the California Consumer Privacy Act was the only game in town when it came to state-level, comprehensive privacy legislation. Sure, we saw many other states introduce similar bills, and Washington got close a couple times to passing the Washington Privacy Act. Those all died on the vine, however. In fact, California was the only state after itself to see passage of anything really big, with the California Privacy Rights Act (which amends the CCPA, and is ***not*** a separate, new law) gaining passage in the November 2020 election.

All to which Virginia has recently stepped forward and said, "Hold my … authenticated consumer request." The Virginia Consumer Data Protection Act (or VACDPA, as I prefer to call it) is a comprehensive privacy bill that was just signed into law by Governor Northam on March 2, and shows influences from both the CCPA and Europe's General Data Protection Regulation (GDPR).

What do you need to know about VACDPA, beyond the fact that it's fun to say out loud? Probably the most important fact is that it won't go into effect until **January 1, 2023**. That gives entities a long runway to understand their obligations under the law and get into compliance.

So, what about all the other stuff? Well…

The Basics

To Whom Does the VACDPA Apply?

SUBSCRIBE

ARCHIVE

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Colman McCarthy
Partner
816.559.2081
cdmccarthy@shb.com

For-profit entities doing business in Virginia are covered by the new law if they control or process personal data of 100,000 Virginia residents in a calendar year. That threshold drops to 25,000 if the business derives over 50% of its gross revenue from the sale of personal data. **Unlike the CCPA, there is no revenue trigger.** So the law can capture small companies that process a lot of data, but pass over medium or large companies without substantial business in Virginia.

Who is left outside the scope of the VACDPA? Notably, public agencies, non-profits and institutions of "higher education." But also—and this is potentially quite impactful—any "financial institution or data ***subject to***" Gramm-Leach-Bliley, or "covered entity or business associate ***governed by***" HIPAA. Those seem to provide entity-wide exemptions, rather than limiting the scope of the exemptions to the data actually covered by those laws.

The Controller/Processor Divide

After the CCPA's exciting creation of the defined terms "business" and "service provider" to distinguish between entities (and to confuse everyone who doesn't have the time to memorize those definitions), the VACDPA has returned to the GDPR's use of the terms "controller" and "processor," and basically adopts the same definitions.

Unsurprisingly, the VACDPA's obligations (disclosures, complying with requests, data minimization, etc., etc.) largely fall on the controller. The processor's obligations generally are to adhere to its contract with the controller and to assist the controller with its obligations. But, as with the GDPR, an entity may occupy both roles, which is a fact-based determination based on the context surrounding a particular instance of processing.

What Information Is Covered?

Like the GDPR, Virginia's new law uses the term "personal data," rather than the CCPA's "personal information." Why point this out? Perhaps out of annoyed frustration at having to use separate terms when trying to keep a written analysis of the law under the length of a novella. For expediency's sake, I'll use the composite term "personal data/information"—or PD/I, for those who share a love for acronyms. (Mostly because the portmanteau "personal datmation" would cause more confusion than most legal terms, and sounds like a breed of dog in any event.)

Notwithstanding the above (probably pointless) digression into legal-term utilization, "personal data" under the VACDPA is defined to include "**any information that is linked or reasonably linkable to an identified or identifiable natural person**." The exact language of that definition differs from what's used in the GDPR and CCPA, and one could write an entire article analyzing the potential implications of those differences. To prevent any sudden attacks of somnambulism, however, I'll simply note for now that—like the GDPR and CCPA—this is an extremely expansive concept of what information can qualify as PD/I.

PD/I does not include de-identified or publicly available information. And the VACDPA includes a host of other exemptions for PD/I covered by other laws, such as HIPAA, the Fair Credit Reporting Act, Driver's Privacy Protection Act, Family Educational Rights and Privacy Act and others.

Also excluded under Virginia's law is PD/I of employees, job applicants, agents or independent contractors in the context of their roles as such. That exclusion is accomplished in two ways, both as a specific exclusion to the law's scope and in the definition of "consumer," which explicitly carves out individuals "acting in a commercial or employment context."

What Other Information Is Covered?

But wait, you say. Isn't there also a definition for "sensitive data?" Yes, there is. PD/I revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status is all considered sensitive data. Joining that information is precise geolocation data (which has its own definition), PD/I collected from a known child (i.e., under 13 years old), and the processing of genetic or biometric data (also with its own definition) for the purpose of identifying a "natural" person (sorry, "legal" persons). This distinction between regular PD/I and sensitive data pops up in connection with one of the rights granted by the VACDPA and with the requirement to perform data-protection assessments.

What Are the Basic Consumer Rights?

The law specifically enumerates five (six? eight? nine?) particular consumer rights:

1. The right to confirm whether a controller is processing PD/I and to access it. (Does that count as two rights?)
2. The right to correct inaccuracies.
3. The right to delete.
4. The right to obtain a copy of the PD/I in portable format.
5. The right to opt out of processing for purposes of targeted advertising, sale of PD/I, or profiling that produces legal or other significant effects concerning the consumer. (That's technically three rights, right?)

Exercise of those rights follows the CCPA's structure. Controllers must provide one or more methods for submitting requests, and must respond within 45 days (extended by 45 days, if necessary) to authenticated requests. Denial of a request requires an explanation, consumers can request information for free twice annually, and controllers can request additional information if needed to authenticate the request.

Any Other Consumer Rights?

Tucked away in the VACDPA's provisions away from the specifically enumerated rights are two other important rights. First, the law provides consumers a right to consent to the processing of sensitive data (though it's framed as proscription on the controller's ability to do so). The VACDPA defines "consent" much like the GDPR and requires a clear affirmative act showing freely given, specific, informed and unambiguous agreement to the processing of the PD/I.

The law also provides a right for consumers to appeal a controller's refusal to take action on a request, and the controller must respond with a written explanation within 60 days. If the appeal is denied, the controller must provide the individual with an online mechanism that allows the consumer to submit a complaint to the Attorney General.

Other Notable Stuff

Narrow Definition of "Sale of Personal Data"

One quite noteworthy difference between the VACDPA and its CCPA cousin is how the laws approach the concept of selling PD/I. The CCPA, as has been repeated ad nauseam, expands the colloquial sense of "sale" to include any transfer of PD/I "for monetary or other valuable consideration." The VACDPA cuts down substantially on that scope to the exchange of PD/I "for monetary consideration" by the controller to a third party. And like the CCPA, there are various exceptions to the definition, such as disclosing PD/I to a processor. Perhaps the most impactful of those exceptions is for transfers to affiliates of the controller.

Data Minimization and Reasonable Security

Data minimization is not a new concept in the world of privacy and data security. And the VACDPA continues a trend we are seeing of laws explicitly enshrining data-minimization principles. Under the law, controllers must limit collection of PD/I to what's relevant, adequate and reasonably necessary for the purposes it's collected, and must not process PD/I beyond those or compatible purposes without consumer consent.

Reasonable security is also not a new concept to privacy law. Many states have laws that require reasonable security for entities that maintain personally identifiable information (a term that is narrower than "personal data" or "personal information" under comprehensive privacy laws). And some laws such as New York's Shield Act and Massachusetts 201 CMR 17.00 try to provide more detailed guidance. Generally, however, what counts as reasonable security under these laws is frustratingly not clear, and the VACDPA is no exception. It simply requires "reasonable administrative, technical, and physical data security" practices "appropriate to the volume and nature of the personal data at issue." How does one apply that in practice? Well, I happen to know that The Sedona Conference (via Working Group 11) just published last month its Commentary on a Reasonable Security Test, a project headed up by Shook's own Bill Sampson. It's a great resource for anyone trying to figure out that question.

Data-Protection Assessments

Much like the GDPR, certain types of activities and certain types of PD/I require entities to perform impact assessments prior to processing. For the VACDPA, that includes processing for targeted advertising, sale of PD/I or certain instances of profiling. Processing sensitive data also requires an assessment, as well as the catchall obligation to perform an assessment for processing activities that "present a heightened risk of harm to consumers." The law requires a cost-benefit analysis for the assessment and consideration of certain factors, such as the use of de-identified data and reasonable expectations of consumers.

Two important things to remember about these data-protection assessments. First, the obligation is not retroactive, so assessments are only required for processing activities that occur on or after January 1, 2023. Second, the Virginia Attorney General is allowed to request a controller's data-protection assessments, which seems like a pathway to public disclosure of potentially privileged information. But the VACDPA anticipates that issue by shielding assessments requested by the AG from Virginia's FOIA law, and providing that disclosure to the AG is not a waiver of attorney-client privilege or work-product doctrine.

What About Enforcement?

Good question. The Virginia Attorney General has exclusive authority to enforce the VACDPA. Penalties can reach as high as $7,500 per violation, but entities have a 30-day period to cure a violation after receiving written notice from the AG.

There is no private right of action (not even for data breaches, like the CCPA), and the law specifically states that it does not provide the basis for one under the VACDPA “or under any other law.” That likely prevents actions under Virginia’s unfair trade practices law seeking to leverage violations of the CDPA.

Anything Else?

Yes, of course. Even after 1,800+ words, this lengthy piece doesn’t cover every nook and cranny of the VACDPA. There are:

- Other exceptions to VACDPA, such as complying with other laws.
- Particular requirements if you want to use de-identified data.
- Particular requirements for processor contracts.
- Lots of detailed definitions that will likely lead to many scholarly musings on their scope.
- And other things besides.

Hopefully this (interminable) snapshot will help you start digesting the many aspects of Virginia’s new, comprehensive privacy law. But, just like any large meal, there’s only so much that can be comfortably consumed at one sitting.

And, of course, digestion is aided by a long nap. Sweet dreams. You’ve earned it.

SHB.COM

ABOUT | CONTACT | SERVICES | LOCATIONS | CAREERS | PRIVACY

The choice of a lawyer is an important decision and should not be based solely upon advertisements.

Unsubscribe | **Forward to a Colleague** | **Privacy Notice**