March 4, 2021

# Virginia Can No Longer Say Whom It's For Without Consent, Thanks to Its New Comprehensive Consumer Privacy Law

by Jon Neiditz , Vita E. Zeltser

---

Virginia knocked off California's crown as the only U.S. state to have a comprehensive, general consumer privacy law when Governor Ralph Northam signed the Virginia Consumer Data Protection Act ("**CDPA**") into law on March 2, 2021, unless you count Nevada which we warned you would stay in Vegas. The law takes effect on January 1, 2023, matching the effective date of the California Privacy Rights Act ("**CPRA**").

Here is what in-house counsel should do now to be well-positioned for compliance in 2023:

- **Figure out how many Virginians' personal data your organization processes to determine whether the CDPA applies to your organization.** As discussed below, the CDPA applies only to certain for-profit entities based on processing thresholds.

- **Create a compliance plan to make sure that you can say "thus always" to noncompliance.** Required compliance measures will vary greatly for each organization depending on an organization's business model (e.g., whether the organization is a provider or customer of technology services) and whether the organization has complied with the California Consumer Privacy Act ("CCPA") and/or the European Union's General Data Protection Regulation ("GDPR"). While the CDPA has certain unique compliance requirements for which covered organizations should account, CCPA / GDPR-compliant companies may find little to do to become compliant with the CDPA, especially considering that the CDPA is not enforceable through a private right of action.

- **Check the scope of your compliance documents.** Your organization may have prepared internal documents (e.g., data protection impact assessments) and prepared notices or executed agreements (e.g., privacy notices and data protection addenda) to comply with the CCPA and GDPR. Review whether those documents apply only to residents of California or the European Union and amend those documents accordingly for Virginia.

**Scope Based On Processing, Not Revenue**

The CDPA applies to for-profit entities that do business in Virginia or sell products or services into the state, so long as the entity meets one of two processing thresholds:

- Processing the personal data of at least 100,000 Virginia consumers; or
- Processing the personal data of at least 25,000 Virginia consumers and deriving more than 50 percent of revenue from selling personal data (i.e., data brokers).

The CDPA excludes entities regulated by the Gramm-Leach-Bliley Act, and covered entities and business associates as defined under the Health Insurance Portability and Accountability Act. This exclusion from coverage is a departure from the California privacy laws referenced above (CCPA and CPRA), which exclude federally regulated data rather than regulated organizations. The relative narrowness of the CDPA's scope thereby provides compliance reprieve for the federally regulated entities that had to comply with the CCPA and will have to comply with the CPRA in addition to those federal regimes.

The CDPA also excludes de-identified data (data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person) from the law's definition of personal data. Virginia lawmakers incorporated into the law a version of longstanding FTC safeguards for ensuring that data remains de-identified. Under the CDPA, controllers possessing de-identified data must: (1) take reasonable measures to ensure that the data is de-identified; (2) publicly commit not to try to re-identify the data; and (3) contractually require downstream recipients to comply with the CDPA.

**Exclusions for B2B and Employee Personal Data**

Unlike the California privacy laws (CCPA and CPRA), the CDPA defines consumers (the group of data subjects that the statute protects) as Virginia residents acting in an individual or household capacity. That definition expressly excludes persons acting in a "commercial or employment context." To gild the lily, the CDPA contains an additional exclusion to the law's scope for the personal data of job applicants, employees, contractors, emergency contacts, and beneficiary recipients, so long as the personal data continues to be used in that employment or beneficiary context.

**Compliance Documents: DPIAs, DPAs, and Appeals**

*(i) Data Protection Impact Assessments (DPIAs)*

The CDPA requires controllers (the entities that determine the purposes and means of processing) to conduct and document data protection assessments (DPIAs) in the event of any of the following triggering events:

- Processing personal data for targeted advertising;

- Selling personal data;
- Profiling that presents any one of the several risks to consumers enumerated in the CDPA;
- Processing sensitive personal data; and
- Any processing activities involving personal data that present a heightened risk of harm to consumers.

The Virginia Attorney General, moreover, may require a controller to produce a DPIA in the event of an investigation.

*(ii) Data Protection Agreements (DPAs)*

The CDPA requires controllers and processors (the entities that process personal data on behalf of controllers) to enter into Data Protection Agreements (DPAs), the content requirements for which somewhat mirror those arising under the GDPR (e.g., the DPA must establish the nature and scope of the processing as well as the processor's obligations to assist the controller). Just as under the GDPR, controllers (customers) and processors (vendors) are especially likely to negotiate certain mandatory DPA provisions, such as those relating to the (i) controller's right to audit the processor's compliance with the DPA, and (ii) the processor's obligation to return and delete personal data at the end of the provision of the services.

*(iii) Publicly Available Appeals Process*

The CDPA requires controllers to establish a process for consumers to appeal the controller's denial or failure to comply with a consumer's rights request under the law. That appeals process requires an update to each controller's website because controllers must conspicuously post notice of that appeals process. Controllers must also post an online mechanism (if one is made available) through which the consumer may submit complaints to the Virginia Attorney General—so a satisfactory response to consumer complaints is critical for reducing the risk of an enforcement action.

**Consumer Rights**

Generally speaking, the consumer privacy rights that the CDPA creates replicate those arising under the GDPR and the CCPA/CPRA:

- To confirm whether a controller processes the consumer's personal data;
- To correct inaccurate personal data;

- To delete personal data provided by or obtained about the consumer;
- To access personal data in a portable format; and
- To opt-out of profiling, targeted advertising and personal data sales.

The requirement to provide an opt-out of information sales is much narrower than the somewhat equivalent right arising under California law, as the CDPA narrowly defines sales as the "exchange" of personal data for monetary consideration by the controller to a third party. The definition expressly excludes, among other exceptions, affiliate sharing and disclosures to a processor.

The CDPA defining sales as an exchange of personal data, and not merely making personal data "available" to a third party (as is the case under California privacy law), reduces the scope of potential sales under the CDPA. In an online context, a website publisher allowing third parties to collect information (that the publisher may never receive) on a website is more clearly "making information available" (and thereby a potential sale under California privacy law) than an "exchange" of information (and therefore not likely a sale under the CDPA).

**Good News for Affiliate Sharing**

Affiliates sharing will require much less analysis under the CDPA than that issue received under the CCPA. The CDPA exempts sharing personal data with affiliates from the law's definition of "selling." Affiliates, under the CDPA, are entities that share common control or common branding (whereas the CCPA requires entities to have both common control and common branding in order to qualify as one business and therefore take the applicable sharing outside of the CCPA's definition of sale).

**Consent is Required for Processing Sensitive Personal Data, but Exceptions Mitigate Operational Burdens**

Controllers must obtain a consumer's consent before processing sensitive personal data, defined to include, among other categories, geolocation information, biometric information, sexual orientation, religious beliefs, and children's personal data. That requirement creates operational burdens for controllers, especially those without privity to consumers through which the controller may collect a consent. Such controllers, however, can approach that requirement by either (i) looking to the CDPA's exceptions to remove the processing from the CDPA's scope (e.g., the law exempts processing for fraud detection, which is a common use case of biometric information) or (ii) requiring contractual counterparties with privity to the consumer to collect a consent on the controller's behalf.

**Privacy Tipping Point?**

Given the legislative activity in other states, it seems that Virginia won't likely be the last state to enact comprehensive privacy legislation this year. The question is whether the passage of such privacy laws will finally push Congress to enact federal privacy legislation. If the state laws passed are as relatively business-friendly as Virginia's CDPA, such laws may not prove to be as unmanageable as many feared. In reality, and thus far, it seems that California's privacy law will likely remain the high bar against which most U.S. companies measure their privacy programs against, and that a comprehensive federal data protection law in 2021 remains unlikely.