June 28, 2021

Top Operational Impacts of Virginia's New Privacy Law (CDPA)

David Manek

Ankura Cybersecurity & Data Privacy

+ Follow Contact

The Virginia Consumer Data Protection Act (CDPA) overwhelmingly passed both legislative chambers this month and is expected to be signed by the Governor in the coming weeks with an effective date of January 1, 2023. Best described as a sibling of the GDPR and cousin of the CCPA, the commonwealth's law borrows on some core themes from the European law including data protection assessments, treatment of sensitive data, consent management, data minimization and delineating of contracting parties as controllers and processors. Like the CCPA, the Virginia law includes obligations related to sales of personal data, though the Virginian definition of sale is more restrictive to cases where a financial transaction occurs. Like both of these laws, and most other privacy regulations around the globe, requirements for data processing transparency in the form of privacy notices and consumer right are also included. An advanced twist is that the law reflects a maturing level of education of legislators on the processing of personal data for targeted advertising via cookies and AdTech, which we will describe further. While this represents another line item in what is becoming a burdensome patchwork of privacy laws, and though the benchmark for what qualifies as "reasonable" security will surely be debated, the Virginia law does offer some guidance in the text which directs efforts around topics such as data protection assessments that have been missing from similar laws.

Scope

According to the text, the law is applicable "to all persons that conduct business in the commonwealth and either control or process personal data of at least 100,000 consumers or derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers". Covered individuals are *residents* of Virginia and any personal data which makes them *identifiable*. This means that even when the information alone may not directly identify an individual, if the organization has reasonably available means to link the data with other records to produce an identity, it may be in scope.

Exemptions

The CDPA does expand upon exemptions from CCPA to include more entity-level carve-outs for businesses such as financial institutions subject to the Gramm-Leach-Bliley Act as well as covered entities and business associates governed by the HHS under HIPAA and HITECH. The concept of being truly covered by HIPAA, as opposed to simply aligning with it as a standard, will likely leave some information in flux of scope. Additionally, specific types and uses of information are exempt such as personal data subject to existing privacy laws governing clinical trials, patient safety, credit reporting and worthiness. Virginia's law also learned from the debates around GDPR and CCPA by exempting employment data, information used to administer benefits, and personal information used in a B2B commercial context.

Key Operational Impacts

1. **Data Protection Assessments:** The requirement for Data Protection Assessments (DPAs, certainly now to be confused with Data Protection Addendums) is what immediately stands out in the CDPA as one of the most significant impacts. This will be new for organizations who have only tackled CCPA but are similar to the Data Protection Impact Assessments (DPIAs) in GDPR's art. 35. DPAs are required under the CDPA for certain processes which are deemed to be higher risk and require a documented evaluation of the risks the processes introduce as well as the controls and remediation plans to mitigate and manage those risks. One welcome difference from the GDPR is that Virginia's law does provide guidance on the specific activities which require a DPA, which include targeted advertising, sales of personal data, certain types of profiling, processing sensitive personal data (more below), and then a more subjective requirement for processes "that present a heightened risk of harm to consumers". Some notes which may help ease the burden include that a single DPA may be conducted for multiple, similar processes and where a similar assessment (potentially DPIA under GDPR) has already been conducted, it may be sufficient to refer to the prior assessment and not require a new DPA. Incredibly important to note is that the Attorney General may request controllers of personal data make the assessments available for review in order to evaluate the level of compliance. This is a significant investigative sword for the AG and underlines the importance of developing a thoughtful, defensible, and actionable process.

2. **Cookies and AdTech:** Virginia's law includes a new definition which is not directly addressed in other laws for *Targeted Advertising,* defined as "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from a consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests." The use of cookies and AdTech processes will absolutely need to be evaluated under CDPA purely based on its inclusion in the list of activities requiring a documented DPA but also because the CDPA includes requirements that individuals be able to opt-out of such advertising. Additionally, organizations must disclose when these processes include any sales of personal data. While

the GDPR largely referred to the ePrivacy Regulation on these matters, and where the CCPA did not directly address targeted advertising, Virginia's bright and clear call out on this topic makes it apparent that legislators are becoming more educated on the workings within the AdTech ecosystem and looking to regulate further. In short, get those cookie banners ready, make sure they are accurate, and that they actually work.

3. **Privacy Notices:** In no surprise, the concept of transparency is at the heart of the CDPA. Controllers of personal data must provide consumers with a privacy notice that identifies the categories of data they process, purposes of the process, a mechanism to exercise their rights, and categories of data shared with third parties. Where applicable, a disclosure of sales of personal data must be made as well. The *categories* of personal data are not defined in the CDPA as they are in other laws which is likely to cause some confusion and solicitation of guidance. We have already seen California Attorney General use these required externally-facing disclosures as easy sources to target for cursory reviews of an organization's efforts towards compliance. The disclosures around the type of data processed and categories of parties with whom it is shared can potentially have large impacts in the event of a data breach if the information exposed is discovered to be in conflict with what the public notice states. This underlines the necessity to be thoughtful when creating and updating these privacy notices and balance between the required specifics and defensible generalizations.

4. **Consumer Rights:** Another expected but potentially impactful inclusion is the concept of consumer rights. This includes the rights to request confirmation whether a controller is processing their personal data, correction of inaccuracies, deletion, obtaining copies or access to the data, and opting out of processes such as targeted advertising, data sales, and certain types of profiling. Responses must be made "without undue delay" and in the latest 45 days. The CDPA also requires that a mechanism for appealing a refusal which must be clearly and inconspicuously posted along with instructions for lodging a complaint to the Attorney General. The law allows for exception flexibility here where the data can be de-identified, and even scrubbed under the less conservative definition of pseudonymized.

5. **Sensitive Data and Consent:** Like the GDPR, and unlike CCPA, the Virginia law includes a definition for sensitive data which is a subset of personal data including anything revealing things such racial and ethnic origin, religious beliefs, health diagnoses, sexual orientation, citizenship or immigration status, genetic data, biometric data, and precise geolocation. This also includes any personal data collected from a known child. Organizations need to identify where such data is processed as it requires the individuals consent as well as the documentation of a data protection assessment. The standard for consent under the CDPA is "a clear affirmative act signifying a consumer's freely given,

specific, informed, and unambiguous agreement to process personal data relating to the consumer." Read that as NO assumed consent (e.g. "by proceeding you give your consent") and no pre-ticked check boxes. Organizations will need mechanisms in place to track consent, particularly parental consent for those under 13. Existing parental consent processes are sufficient so long as they are aligned with COPPA.

6. **Data Minimization and Security:** The CDPA requires organizations only process personal data which is "Adequate, relevant, and limited to what is necessary in relation to the specific purposes". Organizations will need to evaluate whether the information they collect is strictly necessary to achieve the business purpose and not retain such information longer than necessary for business or legal purposes. Like other privacy laws, personal data must be protected with what the CDPA refers to only as "reasonable administrative, technical, and physical" measures. As expected, there are no standards established to what is *reasonable* security. Privacy and information security teams will need to collaborate and document the existing cyber risk management frameworks (e.g. NIST, ISO, CIS Top 20, etc.) and process for reviewing the controls applied and accountability for ongoing evaluation and maintenance of those controls.

7. **Third Party Management:** The CDPA borrows on the GDPR's terms for delineating between *controllers* who determine the means and purpose of the processing and *processors* who strictly access and use the information under direction of the controller. The CDPA requires contracts between controllers and processors to clearly set forth the instruction for processing the data, ensure that the data is subject to confidentiality, require processors to return or delete data upon instruction from the controller, require processors to provide demonstrations of compliance, and in some cases allow the controller to conduct an audit of their programs. Controllers will need to evaluate their third-party relationships, categorize them based on the type of personal data they collect, update contracts with processors as necessary, and potentially enhance processes for vendor due diligence not only leading up to new vendor on-boarding, but also through on-going monitoring across the vendor lifecycle. For processors, it will be important to develop documentation which can support statements on compliance and reduce the friction for drawn-out audits.

Fines and Enforcement

As for the usual scare tactics, the CDPA does not include the private right of action even for cases of a breach. The Attorney General may initiate actions and fines of $7,500 per violation, which we can expect to be interpreted as instances where a single act (e.g. an inaccurate privacy notice) may result in multiple individual violations. The CDPA also creates the Consumer Privacy Fund where such fines will be credited and used to support the work of the Attorney General in enforcing the law.

What to do next?

Depending on how much an organization has or has not done previously for GDPR and CCPA, your impact may vary. At a minimum, organizations should begin with the following activities to kickoff the compliance roadmap:

1. Develop a framework for compliance and controls and map Virginia obligations to other laws such as the GDPR and CCPA.
2. Review, update, or create an inventory of personal data processing activities, assets, and vendors which includes a process to identify sensitive personal data.
3. Extend or implement a process for conducting data protection assessments.

Originally Published on Linkedin.com - February 24, 2021.

✉ Send Print ⚠ Report

RELATED POSTS

- **Using the NIST Privacy Framework to Assess Privacy Risk and Build a Privacy Program**
- **Privacy Considerations in Debt Refinancing and Equity Seed Funding – Are you prepared?**

LATEST POSTS

- **Overview of California AG's Examples of CCPA Non-Compliance**
- **Implementing the NIST Privacy Framework – Govern Function**
- **Colorado Privacy Act: Another Piece to the Data Privacy Puzzle**

See more »

WRITTEN BY:

ankura

Ankura Cybersecurity & Data Privacy

Contact + Follow

David Manek

PUBLISHED IN:

Adtech	+ Follow
California Consumer Privacy Act (CCPA)	+ Follow
CDPA	+ Follow
Cookies	+ Follow
COPPA	+ Follow
Data Privacy	+ Follow
Data Protection	+ Follow
Enforcement Actions	+ Follow
General Data Protection Regulation (GDPR)	+ Follow
Gramm-Leach-Blilely Act	+ Follow
Personal Data	+ Follow
Popular	+ Follow

more ⌄

ANKURA CYBERSECURITY & DATA PRIVACY ON: