March 3, 2021

Step Aside California: Virginia Consumer Data Protection Act Becomes Law

Attorneys
Edward R. McNicholas
Fran Faircloth
Kelsey McIntosh

On March 2, 2021, Virginia Governor Ralph Northam signed the Virginia Consumer Data Protection Act (CDPA) into law without further amendments. Virginia now joins California as the second U.S. state to enact comprehensive privacy legislation. The CDPA will come into effect January 1, 2023 simultaneously with California's Consumer Privacy Rights Act (CPRA). While similar, the laws reflect somewhat differing approaches to a consumer data law, and covered businesses should begin preparing compliance strategies now. In particular, the new Virginia law may well presage movement in other states, such as Washington, New York, etc., or perhaps movement on a federal privacy law. In light of these developments, many clients are shifting away from jurisdiction-specific policies and towards a rationalized national or global approach to privacy and data protection – with local variations as appropriate.

Overview

Since passage of the California Consumer Privacy Act (CCPA) and CPRA, many states have proposed data protection bills that are pushing forward in the legislative process. Virginia's CDPA progressed swiftly and easily in the now "trifecta Blue" Virginia, with the Virginia Senate passing a version of the bill on February 3, less than a week after the House passed a nearly identical companion bill. The bill garnered broad support from both lawmakers and industry. State Sen. David W. Marsden (D-Fairfax), a co-sponsor of the bill, signaled the intention to challenge California and the EU, noting that "Virginia is the world leader in internet traffic" and that the CDPA will enable Virginia to "take[] the lead on protecting consumer data."

The CDPA gives Virginia consumers new rights to access, correct, delete and obtain a copy of the personal information a covered business holds about them, and to opt out of certain data processing activities. Significantly, covered business will also be required to obtain opt-in consent before collecting or processing "sensitive data" and to conduct "Data Protection Assessments" in specified circumstances – a process that is becoming more common but is still deeply embedded only in significantly resourced privacy programs in the U.S..

In terms of enforcement, the CDPA is more business-friendly. Virginia's Attorney General is able to enforce the law with potential fines of $7,500 per violation – which is unclear but may well be argued by the Attorney General as $7,500 per person impacted. On the other hand, the law lacks a private right of action and provisions seen in the CPRA and other proposed legislation that make it easier for individuals to exercise their opt-out rights. While the absence of these consumer-friendly protections has drawn criticism from privacy advocates, it may have made the CDPA more palatable to lawmakers, prompted its speedy enactment, and suggests a path for a federal privacy law.

In contrast to California's CCPA/CPRA, Virginia's CDPA represents a much more common-law approach to implementing a General Data Protection Regulation (GDPR)-like framework that may well fit more comfortably within the U.S. legal structures. While the CCPA tends to take more of a European Civil Code approach, reminiscent of the text of the GDPR, the CDPA incorporates many of the proportionality and reasonableness tests that are the hallmark of the GDPR in practice.

The CDPA's unique framework of rights and obligations will undoubtedly influence bills already percolating in at least eighteen other states. With the looming threat of a patchwork of state laws imposing differing requirements, we expect increased pressure on federal lawmakers to more aggressively pursue national data protection legislation efforts.

Please see below for a summary of key aspects of the CDPA, previously reported on in our DataPhiles blog, that will likely shape future state and federal data privacy legislation.

Applicability and Scope

Covered Entities. Virginia's CDPA applies to "persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth" and that meet either of the following jurisdictional thresholds:

- Annually control or process personal data of at least 100,000 Virginia residents, or
- Control or process personal data of at least 25,000 Virginia residents and derive over 50% of gross revenue from the sale of personal data

Virginia's CDPA's extraterritorial effect echoes that of the EU's GDPR and California's CPRA, but notably Virginia's CDPA applies broadly to businesses that "control or process" personal data, in contrast to California's CPRA's application to a business that "buys, sells, or shares" personal information of 100,000 or more consumers or households. Virginia's CDPA's lack of a gross annual revenue jurisdictional threshold further distinguishes it from California's CCPA and CPRA. This variation in application of the two laws means that it will be important even for businesses that have already evaluated the applicability of the California laws to undertake a similar review for Virginia.

Personal Data. Virginia's CDPA defines personal data broadly, closely hewing to GDPR language, as "any information that is linked or reasonably linkable to an identified or identifiable natural person." Two exceptions are provided for publicly available information and de-identified data. Unlike the California laws, the CDPA does not include information linkable to households, but not to individuals, in its definition of personal data.

Covered Individuals. The CDPA's protections and rights apply to Virginia residents "acting only in an individual or household contexts." Individuals in commercial and employment contexts are specifically excluded, and so there is an inherent employee and B2B exemption.

This difference in coverage is important. It points to the fact that the CDPA is not an omnibus EU-style human rights data protection law as much as it is a U.S.-style consumer protection privacy law.

Obligations for Controllers and Processors

Virginia's CDPA eschews California's somewhat awkward "business" and "service provider" designations in favor of specific obligations for "controllers" and "processors" resonant of the GDPR.

Controllers. The key requirements for controllers (any entity that, alone or jointly, determines the purposes and means of processing) include:

- Providing a privacy policy to consumers describing the entity's information processing practices and consumers' rights;
- Establishing and implementing reasonable data security practices to protect personal data;
- Responding to consumer rights requests; and
- Conducting Data Protection Assessments in certain circumstances.

Processors. Processors (entities that process personal data on behalf of a controller) are generally required to follow the instructions of controllers and to assist controllers in meeting their obligations under the CDPA. Written contracts between controllers and processors, and processors and their sub-processors, will be required prior to processing of personal data.

Data Protection Assessments

Virginia's Data Protection Assessment requirement aligns the CDPA with the GDPR, as well as with the CPRA, which will require cost-benefit risk assessments for certain processing activities. Virginia, however, goes beyond California by requiring a Data Protection Assessment when the processing of personal data constitutes:

- targeted advertising;
- a sale of personal data;
- certain instances of profiling;
- sensitive data; or
- a heightened risk of harm to consumers.

Such Data Protections Assessments will be reviewable by the state Attorney General during an investigation, although they will be exempt from Virginia's FOIA provisions. Accordingly, one might hastily conclude that Virginia's Data Protection Assessment would not be protected by privilege. Virginia's statute makes clear that disclosure of a Virginia Data Protection Assessment would *not* waive attorney work product or attorney-client protections, and federal courts should respect this state demarcation of a privilege. This thoughtful approach to Data Protection Assessments certainly contemplates that these assessments will be performed by counsel and normally subject to work product and privilege protections so as to encourage robust internal communication and consideration of alternatives, such as use of de-identified, synthetic, or pseudonymous data.

Sensitive Data and Opt-In Requirements

"Sensitive Data." The CDPA takes a somewhat European approach to sensitive data by not including financial information. In Virginia, sensitive data would be:

1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
3. The personal data collected from a known child; and
4. Precise geolocation data.

Though these classes of personal information are historically unfamiliar to U.S. law, this broad definition reflects trends seen in the CPRA and proposed Washington Privacy Act, as well as the GDPR.

Consent Requirements. Covered companies must obtain opt-in consent to collect or process sensitive data. Again mirroring the GDPR, consent must be "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement" to the processing. The opt-in requirement for *any* processing of sensitive data is more stringent than that of California's CPRA, which provides consumers only the right to opt out, and may pose challenges to implement in practice.

Virginia's CDPA also requires businesses to obtain opt-in consent before processing personal data for unnecessary or incompatible secondary purposes.

We note, however, that a prior FCC effort to create an opt-in privacy regime was struck down as an unconstitutional intrusion on commercial free speech. *See U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1998).

Consumer Rights and Opt-Out Requirements

Virginia's CDPA provides covered consumers with rights of access, correction, deletion, and portability, as well as the right to opt out of the processing of their personal data for certain purposes. This suite of rights, taken almost exactly from the proposed 2021 Washington Privacy Act, contains two noteworthy points.

First, businesses are exempted from complying with access, deletion, correction, or portability requests for "pseudonymous data" in certain circumstances. Additionally, businesses are not required to re-identify pseudonymized (or de-identified) data in order to comply with any individual request, similar to the GDPR's exemption for pseudonymous data in response to certain data subject requests. Accordingly, covered businesses may consider pesudonymization as a compliance strategy for the CDPA.

Second, Virginia's CDPA's opt-out right is more limited than the global opt-out right of the California CCPA and CPRA, as Virginia grants consumers the right to opt out of processing of their personal data for three enumerated purposes: "(i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." Additionally, the CDPA contains no provision for authorized agents to exercise the right on behalf of a consumer, instead requiring consumers to exercise their rights individually.

Exemptions

Virginia's CDPA provides a long list of entities and data that are exempt from its scope, including certain governmental entities, non-profits, and higher education institutions, as well as information subject to the Fair Credit Reporting Act (FCRA), the Children's Online Privacy Protection Act (COPPA), or other federal laws, and personal data processed in employment contexts.

Interestingly, entity-based *and* data-based exemptions are provided with respect to the Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA). The CDPA does not apply to financial institutions *or* data subject to the GLBA, nor to covered entities or business associates subject to HIPAA. Separately, the CDPA exempts certain personal health information (as defined by HIPAA), patient information, and health records, as well as identifying information processed in certain research contexts and any information derived from these health care exceptions that is de-identified pursuant to HIPAA deidentification requirements. The nuances of these exemptions will require further scrutiny, but the provisions appear to exclude health care organizations as well as considerable amounts of medical research broadly.

Enforcement

The Virginia Attorney General is the only party authorized to institute civil actions against both controllers and processors for violations of the rights and requirements established by the CDPA, subject to a 30-day cure period. In these actions, the AG can assess penalties up to $7500 per violation. Unlike California's CCPA, however, no private right of action is provided in the case of cybersecurity failures, and the text expressly precludes interpretation to support an implied right of action.

* * *

While Virginia is only the second state to enact comprehensive privacy legislation, many other states, including New York, Minnesota, and Washington, have been considering similar bills. We are watching these state developments closely. If you have any questions about this Alert or other privacy law developments, please contact Ropes & Gray's data, privacy & cybersecurity attorneys.