Data Privacy and Cybersecurity

Virginia Set to Become Latest State to Enact Comprehensive Consumer Privacy Law

By: David P. Saunders and Andrew C. Elliott

Having passed major hurdles in both the state house and senate, Virginia's Consumer Data Protection Act (CDPA) is poised to become law. If enacted, the CDPA will become effective January 1, 2023 (the same date the remaining portions of California's Consumer Privacy Rights Act (CPRA) come online). While much of the CDPA tracks the CPRA, there are meaningful differences between the two bills, and CDPA will require companies covered by the new law to implement changes both to their public privacy policies as well as to internal processes.

Who Is Covered By the CDPA?

The CDPA would apply to any person doing business in Virginia and who: (i) processes personal data of at least 100,000 consumers in Virginia annually, or (ii) derives more than 50 percent of gross revenue from the sale of personal data and processes personal data of at least 25,000 Virginia consumers annually. The CDPA will not, however, apply to nonprofit organizations, institutions of higher education, governmental bodies, financial institutions already subject to the Financial Services Modernization Act of 1999, and those covered under certain health care data laws.

What Is Covered By the CDPA?

The CDPA would apply to "personal data," defined as "any information that is linked or reasonably linkable to an identified or identifiable natural person." This definition does *not* include de-identified data and publicly available information. Also exempt from the reach of CDPA is a variety of data categories subject to federal regulation such as health information under HIPAA and educational records under FERPA. Unlike the CPRA, the CDPA does *not* include a list of the kinds of data that constitute "personal data." This absence is particularly noteworthy because the CDPA definition appears, at least on its face, narrower than the CPRA definition, which covers "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked directly or indirectly with a particular consumer or household." Despite these differences, from an operational perspective, it is likely more efficient for businesses to consider the term "personal data" under the CDPA and "personal information" under the CPRA to be equivalent.

Like the CPRA, the CDPA also creates a "sensitive data" categorization that is subject to additional protections beyond mere "personal data." Once again, however, there are differences between the scope of the two laws. The CDPA's "sensitive data" categorization only applies to a person's ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship, immigration status, precise geolocation, genetic or biometric information, and information collected from a known child. "Sensitive Data" under CDPA can only be processed by a business if the business obtains express consent from the consumer.

Who Has Rights Under the CDPA?

The CDPA would give rights to data subjects who are "resident[s] of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context." This definition is important for what it does not cover. Unlike in California, where "households" have rights under the CPRA, "households" do not have individual consumer rights under the CDPA. Additionally, like the CPRA, there is a carve-out to the rights of individuals such that employees and others acting in a commercial context (*e.g.,* business contacts) do not have consumer rights under the CDPA. The key difference between the CDPA and CPRA is that the CDPA's exemption for employee and business data does not sunset.

What Rights Do Consumers Have Under the CDPA?

In keeping with other global privacy legislation enacted in recent years, the CDPA would establish a set of rights that consumers could exercise with respect to their data:

1. The right to confirm whether a controller is processing the consumer's data, and to access such personal data;

2. The right to correct inaccuracies in data collected;

3. The right to delete personal data provided by or obtained about the consumer;

4. The right to obtain a copy of personal data the consumer has previously provided to the business in a portable format that allows the consumer to transmit the data to another controller; and

5. The right to opt out of a businesses' processing of personal data if used for targeted advertising, sold, or used in profiling the consumer in ways that inform decisions which produce "legal or similarly significant" effects.

Businesses have up to 90 days (including one 45-day extension) in which to respond to a verified consumer request to exercise one of these rights. Consumers can make requests for free up to twice a year under the CDPA. However, a business can charge for subsequent requests or those that are "manifestly unfounded, excessive, or repetitive." A business also need not comply with a consumer request if the requestor's identity cannot be validated. New in CDPA, however, is that a business that does not act on a consumer's verified request must permit the consumer to appeal that decision (more on that below).

What Changes Must a Business Make to Comply With CDPA?

It seems like a Sisyphean task sometimes, but businesses will once again need to update both their external privacy policies and internal procedures to comply with a new data privacy law in the United States. Jenner & Block is preparing an updated privacy policy checklist to account for these new requirements, but in the meantime, below are some of the major changes that businesses will have to address:

- Appeal Rights. CDPA requires a business to develop an internal appeals process whereby a consumer can challenge a business' refusal to act on a verifiable consumer request. The CDPA is light on details of the requirements of this appeals process other than: (i) it should be similar to the process for submitting a consumer request in the first instance; (ii) the appeals process should conclude within 60 days of receipt of the appeal; and (iii) if the appeal is denied, a business needs to tell the consumer how they can submit a complaint to the Attorney General of Virginia. We assume that the Attorney General will promulgate more rules to further define this process.

- Data Protection Assessments (DPA). What many might call a risk assessment, the CDPA calls a "Data Protection Assessment." The CDPA imposes a requirement on covered businesses to conduct a DPA where personal information is used in connection with: (i) targeted advertising; (ii) a sale of the data; (iii) creation of a consumer profile where the profiling could lead to a risk of harm to the consumer; (iv) processing sensitive data; or (v) any other processing that could lead to a heightened risk of harm to consumers. Businesses have to maintain these DPAs and, if requested, produce the DPAs to the Attorney General.

- Update Privacy Policies. What would a new privacy law in the United States be without requiring businesses to once again update their public privacy policies? CDPA is no exception. Among the changes required by the CDPA are: (i) a description of how a consumer can appeal a refusal to comply with their verified request; (ii) an express disclosure of the fact that a company engages in targeted advertising (if it does so in the first instance); and (iii) businesses must make a public commitment to not re-identify de-identified data. All in all, these changes likely will not require entire overhauls of privacy policies, but they will nonetheless require a business to once more refresh its policies.

- Update Service Provider Contracts. Like the CPRA, the CDPA imposes an obligation on businesses to enter into contracts with service providers that limit the service provider's use and further distribution of the personal data that it receives. However, the CDPA introduces a new concept: a service provider must also promise in a contract not to attempt to re-identify data that has been de-identified.

Despite all these changes, the good news for businesses is that the CDPA preserves many of the business-use exemptions present in the CPRA. For example, the CDPA does not prevent businesses from using personal data for the purposes of preventing fraud, troubleshooting products, or complying with a business' other legal obligations.

What Are the Enforcement Mechanisms?

The Attorney General of Virginia has the exclusive authority to enforce the CDPA. The CDPA expressly provides that it

does not create, nor can it be used as, the basis for a private right of action. CDPA also contains a cure provision. Before being fined by the Attorney General, a business will receive a written notice of an alleged violation. The business then has 30 days to cure the violation and provide a statement indicating no further violations will occur. Ultimately, violations could result in civil penalties of up to $7,500 each.

Contact Us

David P. Saunders

dsaunders@jenner.com | Download V-Card

Andrew C. Elliott

aelliott@jenner.com

Meet Our Team

Practice Leaders

David Bitkower

Chair

dbitkower@jenner.com

Download V-Card

David P. Saunders

Co-chair

dsaunders@jenner.com

Download V-Card