AUGUST 18, 2022 | STATE & LOCAL TRENDS

Preparing for the Virginia Consumer Data Protection Act

Beginning June 1, 2023, the Virginia Consumer Data Protection Act (CDPA) will come into effect for Virginia businesses and consumers.

What is the CDPA?

At its core, the CDPA is a data privacy law intended to provide guardrails on how businesses use and store the data of Virginia consumers. Virginia was the second state to pass a state data privacy law after California's California Consumer Privacy Act (CCPA).

The CDPA will apply to covered businesses that conduct business in Virginia or affect Virginia commerce through targeting products and/or services to Virginia residents. For the CDPA to apply to a company, it must either:

- Control or process the personal data of at least 100,000 consumers during a calendar year; or
- Process the personal data of at least 25,000 consumers and derive more than 50 percent of their gross revenue from selling personal data.

Personal data in this context includes "any information that is linked or reasonably linkable to an identified or identifiable natural person."

What are the CDPA requirements?

The CDPA draws on concepts from the California Privacy Rights Act, CCPA, and the General Data Protection Regulation (GDPR) by establishing consumer rights relating to Privacy.

The main areas of the CDPA that businesses should prepare for are as follows:

- **Access Rights:** Consumers will have the right to know whether a business is processing their personal data and, the right to access that data if so. Consumers will be able to make data access requests, to which businesses must either: respond in 45 days, request an extension, request more information relating to the request if necessary, or refuse the request if it's not "commercially reasonable" to comply with.

- **Data Portability:** Consumers will have the right to obtain a copy of the personal data they have provided to a business in transferrable form.
- **Consent:** Consumers must be made aware of what data businesses use and how, though consent is not required in most cases. Businesses would need consumer consent if they decided to use already collected personal data for a new purpose or want to use sensitive personal data (A diagnosis of physical or mental health, any personal data that is about a child, genetic or biometric data that identifies somebody, information about ethnic or racial origin, information about immigration status or citizenship, information about religious beliefs, information about sexual orientation, or precise geolocation data).
- **Right to Correct:** Consumers will have the right to correct any inaccuracies in the personal data a business holds about them. The CDPA indicates that this right takes "into account the nature of the personal data and the purposes of the processing of the consumer's personal data." So, it is possible that enforcement around this particular right could depend on guidance from the Attorney General.
- **Right to Delete:** Consumers will have the right to demand that a business delete the personal data it holds about them. However, the law has not yet established how long a company has to comply with such a request.
- **Right to Opt-Out:** Consumers will have the right to opt-out if companies: (1) sell their data; (2) use their data for targeted advertising; or (3) use their data for profiling.
- **Right to Exercise Rights**: Businesses will be unable to discriminate against a consumer who exercises any of their CDPA rights by refusing to service the customer, charging higher prices to the consumer, changing their terms of service, or threatening to do any such thing.
- **Privacy Policy:** Businesses must publish a privacy notice or privacy policy.
- **Data Protection Assessments**: The CDPA requires that companies conduct data protection assessments if they intend to: process personal data for profiling that could harm the consumer; process sensitive personal data; process data in a way that creates a "heightened risk of harm" to the consumer; sell personal data; or use personal data for targeted advertising.

Are there any exclusions to the CDPA?

The CDPA differs from the CCPA in that it excludes employee data from its coverage, potentially because CCPA's coverage of workplace data was confusing and difficult to implement. The CPPA, for reference, mandated that covered employers provide notice and a variety of data privacy rights to employees, job applicants and independent contractors when personal information was collected for employment, recruitment and contracting purposes.

The CDPA excludes anonymized data or publicly available information from its coverage, and also specified that certain entities and types of data are exempt from coverage. The following entities are excluded from coverage:

- A body, authority, board, bureau, commission, district or Virginian agency, or any Virginian political subdivision.
- Any financial institution or data covered by the Gramm-Leach-Bliley Act (GLBA).
- Entities that are subject to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act.
- Nonprofit organizations.
- Higher-education institutions.

How is the CDPA enforced?

The CDPA does not contain a private cause of action, and the Virginia attorney general is the sole enforcer of the law. If violations are found, businesses are afforded 30 days to correct any violation. If a business doesn't meet that deadline, then the Virginia Attorney General can issue a civil penalty of $7,500 per violation. Each person whose consumer rights have been violated would count as an individual violation – meaning it would be easy for penalties to accumulate quickly to substantial amounts for employers that are not conscientious about compliance.

Businesses should be mindful of the CDPA coming into effect next year, as compliance could be both burdensome and challenging for businesses who are not prepared in advance.