ECKERT SEAMANS
ATTORNEYS AT LAW

March 8, 2021

Data Security & Privacy Alert

Virginia Imposes New Data Protection Requirements on Businesses: Lessons Learned

By Sandy B. Garfinkel, Stephenie Scialabba, and Shannon Kapadia

On March 2, 2021, the Governor of Virginia signed into law the nation's second comprehensive consumer privacy law, the Virginia Consumer Data Protection Act ("VCDPA"), effective January 1, 2023.

The world was introduced to sweeping privacy regulation in 2018, when the EU's landmark privacy law known as "GDPR," short for General Data Protection Regulation, came into effect. California quickly followed suit, enacting the California Consumer Privacy Act ("CCPA"), which became effective in January of last year. By the end of 2020, CCPA was significantly enhanced by a referendum vote on the California Privacy Rights Act ("CPRA"). The VCDPA contains a number of features found in GDPR and CCPA, along with several significant differences. The following are some of the key features of this law:

1. The VCDPA only applies to businesses (referred to as "Controllers") that either:
    a) control or process Personal Data of at least 100,000 "Consumers"; *or*
    b) (i) derive over 50% of gross revenue from the sale of Personal Data *and* (ii) control or process Personal Data of at least 25,000 Consumers

    ❖ Importantly, "Consumers" is defined to exclude persons acting in a commercial or employment role.

2. Controllers are required to provide Consumers with at least one secure, reliable method to invoke the following Consumer rights:
    a) Confirmation on whether the Controller is processing their data
    b) Access to their Personal Data being processed
    c) Correction of inaccuracies with their Personal Data
    d) Deletion of Personal Data provided by or obtained about the Consumer in certain circumstances
    e) Obtain a copy of their Personal Data
    f) Opt out of the processing of their Personal Data for purposes of targeted advertising, sale, or profiling done in furtherance of decisions that may produce legal effects concerning the Consumer.

3. Controllers have several responsibilities under this law, including obligations of transparency, security, and limitation. For instance, Controllers must limit the collection of Personal Data to only that which is "adequate, relevant and reasonably necessary" for the disclosed processing purposes. Additionally, Controllers must establish a process for Consumers to appeal a denial of a rights request. A subsequent denial must include a method for a Consumer to contact or complain to the Attorney General.

4. Controllers must provide Consumers with a Privacy Notice addressing the categories and purposes of Personal Data processed by the Controller, how Consumers may exercise their rights, and the categories of Personal Data shared with Third Parties (also categorized). Additional obligations exist if a Controller sells Personal Data or uses it for targeted advertising.

5. Controllers must conduct and document Data Protection Assessments when performing certain types of processing. The assessments must identify and weigh benefits to the Controller, Consumers and the public against risks to Consumers' rights. Assessments will only be required for processing activities conducted after January 1, 2023 and are not retroactive.

6. Controllers must enter into agreements with data "Processors" that: (a) clearly set forth instructions for processing Personal Data; (b) identify the type of Personal Data subject to processing, the duration of processing, and the rights and obligations of both parties; and (c) ensure that individuals processing Personal Data are subject to a duty of confidentiality. These agreements must also provide for the deletion or return of data at the request of the Controller or termination of the relationship. Any subcontractors that are engaged must meet the statutory obligations for Processors.

7. Controllers must obtain Consumers' consent (defined as a written or an otherwise unambiguous action signifying the Consumer's specific, informed and freely given agreement) before processing "Sensitive Data." Sensitive Data includes:

    a) Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;

    b) Genetic or biometric data processed for the purpose of uniquely identifying a natural person;

    c) Personal data collected from a "known child" (undefined); or

    d) Precise geolocation data.

LESSONS LEARNED

Thanks to VCDPA's predecessor laws, companies have the benefit of several lessons learned from a compliance perspective:

- Be aware that VCDPA, GDPR or CCPA/CPRA compliance are not equal substitutes; while certain obligations and concepts may overlap, there are some key areas of distinction (*click here to view a comparative table*).

- Be conscious of jurisdictional reach. Many companies voluntarily jumped into CCPA compliance out of fear. While a calculated risk analysis may lead to a conclusion that compliance is required, it may also plausibly produce a conclusion that compliance is **not** required.

- Be flexible and anticipate potential changes. CCPA regulations were revised several times before they were finalized, and many of the changes were significant. The VCDPA does not expressly call for the development of regulations by the Virginia Attorney General, unlike CCPA, but does establish a "work group" of state officials, business representatives and consumer rights advocates to review the law and submit by November 1, 2021.

- Be proactive but don't panic; new comprehensive privacy laws generally give some time to get up to speed before becoming effective allow periods to "cure" violations, and may have a delayed enforcement provision. That said, a last-minute effort for compliance could lead to difficulties, especially where vendors are involved. Start early by evaluating what data you have (including whether it falls into a sensitive category), map the source and how you use or disclose it, and decide whether you really need or want it in light of the accompanying obligations. If necessary, it's never too early to begin gathering vendor contracts that may need to be amended.

- Be mindful of "sensitive" data; sensitive personal data is generally treated differently than other data, with more scrutiny concerning its collection and use, and greater consumer protections than other forms of personal information.

In preparing for VCDPA, companies should also assess whether they will be affected by the new California privacy law, CPRA, and be on the lookout for other states that are considering privacy reforms in the nature of CCPA and VCDPA.

ECKERT SEAMANS ATTORNEYS AT LAW

This Data Security & Privacy Alert is intended to keep readers current on developments in the law. It is not intended to be legal advice. If you have any questions, please contact Sandy Garfinkel at 412.566.6868 or sgarfinkel@eckertseamans.com, Stephenie Scialabba at 412.566.1925 or sscialabba@eckertseamans.com, Shannon Kapadia at 804.647.4676 or skapadia@eckertseamans.com, or any other attorney at Eckert Seamans with whom you have been working.