Simpson Thacher

Memorandum

Virginia Passes Comprehensive New Privacy Law

March 9, 2021

On March 2, 2021, the Virginia Consumer Data Protection Act ("CDPA") was signed into law by Governor Ralph Northam, with an effective date of January 1, 2023.[1] California and Virginia now have their own comprehensive privacy laws, while New York, Washington and other states are considering analogs of their own.[2]

Does CDPA Cover My Organization?

CDPA applies to persons that "conduct business" (not defined) in Virginia or produce products or services that are targeted to Virginia residents and (i) control or process annually the personal data of at least 100,000 Virginia residents or (ii) control or process personal data of at least 25,000 Virginia residents and derive more than 50% of their gross revenue from selling personal data. This differs from the California Consumer Privacy Act ("CCPA")[3], which also covers businesses with more than $25 million in annual revenues, regardless of how much California personal information they handle. So a large U.S.-wide business with a tiny local footprint would be covered by the CCPA, but would not be covered by Virginia's CDPA.

"Financial institutions" (not defined), HIPAA-covered entities and "business associates" are exempt in their entirety from the CDPA, which differs from the CCPA and GDPR on this point. Similar to CCPA, the CDPA exempts any data covered by Title V of the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act and a few other statutes. Not-for-profit organizations and institutions of higher learning are also exempt. The CDPA covers personal information related solely to a Virginia resident's role as an individual or consumer, not as an employee or agent of a covered business. The CDPA does not cover data processing in certain instances, such as compliance with law and law enforcement, activities in connection with litigation, performing a contract with a consumer or responding to security incidents.

[1] Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-571 through 59.1-581.

[2] This memorandum provides only a high-level summary of the CDPA. For a more detailed discussion, please consult one of the authors of this memorandum. More information on the CCPA can be found in previous memoranda: https://www.stblaw.com/about-us/publications/details?id=db56f20e-743d-6a02-aaf8-ff0000765f2c and https://www.stblaw.com/about-us/publications/details?id=0310f10e-743d-6a02-aaf8-ff0000765f2c.

[3] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199.

Does My Organization Already Comply?

If your organization is currently subject to and complies with the CCPA, which applies to data of California residents collected after Jan. 1, 2020, and the European Union's General Data Protection Regulation ("GDPR")[4], which took effect on May 25, 2018, then it already substantially complies with Virginia's CDPA, because your organization should already: (i) make multiple disclosures about how and why your organization processes and discloses personal data; (ii) have in its privacy policy a statement on consumer "opt out" rights in certain circumstances; (iii) use reasonable data security practices; (iv) not collect or process personal data unnecessarily or discriminate against consumers in any state for exercising their legal data rights; (v) conduct impact assessments for covered data processing activities; (vi) include data privacy terms in its relevant vendor contracts; and (vii) have a system to respond to consumer requests regarding personal data and have contact information in its privacy policy.

What Else Is to Be Done?

The CDPA has a few new obligations that are not covered by the CCPA, so covered companies will need to update their privacy practices with respect to Virginia-based personal data collected after January 1, 2023[5]:

- Conduct a "data protection assessment" (similar to the data protection impact assessments required under the GDPR) relating to any: (i) processing of personal data for targeted advertising; (ii) sale of personal data; (iii) processing of personal data for profiling or otherwise, where there is a reasonably foreseeable risk of harm to consumers; or (iv) processing of sensitive data;
- Not process "sensitive data" (*e.g.*, data relating to race, ethnic origin, religion, health, sexual orientation, citizenship or immigration status, genetic or biometric data, geolocation data or data relating to children) without opt-in consent (the GDPR has a similar requirement for "special categories of personal data," and the CPRA will introduce new rules regarding sensitive data processing);
- Have a contract between the data controllers and processors (with provisions substantially similar those cited in the CCPA and/or GDPR) that lays out the parties' obligations with respect to personal data;[6] and
- Take reasonable measures to ensure that any de-identified data cannot be associated with a natural person and publicly commit to the same.

---

[4] EU General Data Protection Regulation (Regulation (EU) 2016/679).

[5] The California Privacy Rights Act ("CPRA"), Cal. Civ. Code §§ 1798.100-1798.199, which was passed by ballot initiative in November 2020, also takes effect on Jan. 1, 2023 and covers data collected as of Jan. 1, 2022. Therefore, companies should update their compliance practices with both statutes in mind.

[6] The CPRA has updated the language required in a data processing agreement for the processor to qualify as a "service provider" under the statute. Meanwhile, the European Commission recently published proposed drafts for new standard contractual clauses for the transfer of personal data to third countries, which are expected to be approved within the next several months. To be efficient, any updated data processing agreements should use language that simultaneously complies with the CDPA, CPRA and GDPR.

There is no private right of action for CDPA violations, whereas the CCPA has a private right of action in the specific context of security breaches affecting unencrypted data. The Virginia Attorney General ("AG") may bring actions for violations of CDPA and seek damages of up to $7,500 for "each violation" (which is not defined and could mean each affected consumer) that is not cured by a covered business after 30 days' written notice.

For further information regarding this memorandum, please contact one of the following:

NEW YORK CITY

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Bobbie Burrows
+1-212-455-2333
bobbie.burrows@stblaw.com

Jonathan S. Kaplan
+1-212-455-3028
jonathan.kaplan@stblaw.com

Alysha J. Sekhon
+1-212-455-3762
alysha.sekhon@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Amy Gopinathan*
+1-212-455-7088
amy.gopinathan@stblaw.com
**Not Yet Admitted*

Jacob Lundqvist
+1-212-455-3348
jacob.lundqvist@stblaw.com

Genevieve Dorment
+1-212-455-3605
genevieve.dorment@stblaw.com

Melanie D. Jolson
+1-212-455-3346
melanie.jolson@stblaw.com

Kate E. Mirino
+1-212-455-2055
kate.mirino@stblaw.com

PALO ALTO

Harrison J. (Buzz) Frahn
+1-650-251-5065
hfrahn@stblaw.com

Amber R. Harezlak
+1-650-251-5262
amber.harezlak@stblaw.com

Corina McIntyre
+1-650-251-5073
corina.mcintyre@stblaw.com

WASHINGTON, D.C.

Vanessa K. Burrows
+1-202-636-5891
vanessa.burrows@stblaw.com