wiley

NEWSLETTER

Five Considerations for Navigating Privacy Compliance Under Virginia's and California's New Laws

May 2021

Privacy In Focus®

In March 2021, with the passage of the Consumer Data Protection Act (CDPA), Virginia took its place as the second state to enact comprehensive data privacy legislation. Virginia follows California, where voters recently approved the Consumer Privacy Rights and Enforcement Act (CPRA), which amends that state's existing omnibus privacy law, the California Consumer Privacy Act (CCPA). While neither the CPRA nor the CDPA takes effect until January 1, 2023, there are important steps that a business can take now to plan their compliance consistently across both frameworks.

Virginia's new framework shares similarities with both California's existing CCPA and the new CPRA. But businesses should pay close attention to five areas where Virginia diverges from California and adjust their compliance programs accordingly.

1. **Expanded Consumer Right to Opt-Out**

Both state regimes offer consumers the ability to opt-out of the sale of personal information. Notably, the CCPA provides consumers with the ability to opt-out from the sale of personal information, with the term "sale" being broadly defined to encompass essentially any exchange of a consumer's personal information by a business to a third party for monetary *or other valuable* consideration.

While the CDPA regime takes a narrower approach to the definition of "sale," limiting it to exchanges with third parties for *monetary consideration* only, it takes a broader approach to the right to opt-

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
State Privacy Laws

out, extending the right to include opt-out of processing of personal data for purposes of (1) targeted advertising, or (2) profiling in furtherance of decisions that produce legal or similarly significant effects, in addition to the sale of personal data. So, businesses that are subject to both the CCPA and the CDPA will need to expand their opt-out mechanism in light of Virginia's new law. At the same time, businesses that already comply with the CCPA will have to expand their approach to account for the CPRA's changes to the California opt-out right, which include broadening it to apply to businesses sharing personal data for cross-context behavioral advertising.

2. New Consumer Right to Correction

The new Virginia law establishes a new consumer right to correct that is not found in the CCPA. Specifically, controllers must comply with an authenticated consumer request to exercise the right to "correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data." This is also a new right under the CPRA, which amends the CCPA to establish a consumer right to correct inaccurate personal information that a business maintains. Under the California law, a business collecting this personal information must, among other things, "use commercially reasonable efforts" to correct the inaccurate personal information upon receiving a verifiable request, and in doing so, businesses may also "tak[e]" into account the nature of the personal information and the purpose of the processing of the personal information. Importantly, the right to correction will be the subject of one of the many rulemakings set to take place in California in the coming year. Businesses subject to both the Virginia and California frameworks may be able to draw from that rulemaking process as they build a compliance program with a right to correction that will satisfy both state regimes.

3. Required Consumer Appeals Process

The CDPA diverges from both the existing CCPA and the amended CPRA in that it mandates that a controller must establish a "conspicuously available" process for a consumer to appeal the controller's decision not to take action on a consumer request. Within 60 days of receipt of an appeal, a controller must provide a consumer with a written decision accompanied by an explanation of the reasons for the decision. If the appeal is denied, the controller must also provide the consumer with a means to contact the Attorney General to submit a complaint. While the California framework requires a business to disclose any rights the consumer may have to appeal a decision by a business, it does not *require* that businesses offer this appeal right.

4. New Consent Mechanisms for Sensitive Data

The Virginia law, as well as the CPRA, goes further than the existing CCPA in its treatment of "sensitive data." Where the existing CCPA does not define "sensitive" data, and does not create heightened requirements for such data, the CDPA and CPRA each have distinct frameworks with respect to sensitive data. The definition of "sensitive data" is different under the CDPA and the CPRA, as are the consent requirements that are triggered by the collection and processing of sensitive data. In Virginia, a controller will need to obtain affirmative opt-in consent to process such data, and in California, businesses will need to offer consumers the right to limit a business's use of the consumer's sensitive personal information to that use "which is necessary to perform the services or provide the goods reasonably expected by an average consumer."

Businesses will need to assess whether data they collect will be considered "sensitive data" under these regimes and adjust their consent mechanisms appropriately in light of these new obligations.

5. New Data Protection Assessments

Finally, Virginia's new law will require data protection assessments where the existing CCPA is silent on this type of obligation. Specifically, the CDPA requires data processors to conduct and document a data protection assessment of processing activities involving personal data under certain circumstances, including: (1) targeted advertising, (2) sale of personal data, (3) profiling that presents a reasonably foreseeable risk of substantial injury to consumers, (4) processing of sensitive data, and (5) any processing activities involving personal data that present a heightened risk of harm to consumers.

Of note, the CPRA grants authority to the new California Privacy Protection Agency to promulgate regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security to conduct regular risk assessments. It will be important for businesses to monitor this activity closely and to work to align their Virginia compliance programs with their California ones.

Businesses and organizations covered by the Virginia and California laws should keep these five areas top of mind as they anticipate the need for compliance with new requirements by Jan. 1, 2023.