wiley

ALERT

New Year, New State Privacy Laws: California and Virginia Laws Are Now Effective and More Requirements Are on Tap in 2023

January 4, 2023

2023 already is a landmark year for privacy regulation. As of January 1, 2023, two new privacy laws are now in effect: (1) the **California Privacy Rights Act (CPRA)**, which amends the California Consumer Privacy Act (CCPA), and (2) the **Virginia Consumer Data Protection Act (VCDPA)**. And later this year, three additional new privacy laws will become effective: the **Colorado Privacy Act (CPA)** and the **Connecticut Data Privacy Act (CTDPA)** on July 1, 2023, and the **Utah Consumer Privacy Act (UCPA)** on December 31, 2023. As outlined in our U.S. State Privacy Law Guide, these sweeping privacy laws impact a wide range of businesses (and in the case of Colorado, non-profits) that collect or use personal information about individuals residing in the respective states, and impose new and complex requirements.

While businesses have invested significant resources into updating privacy protocols and notices to meet the January 1, 2023 effective date for California and Virginia, there is still more work to be done to ensure covered businesses are ready for 2023 privacy compliance obligations, including the additional state laws and new regulations in California and Colorado.

Compliance requirements for emerging U.S. state privacy laws and regulations can be a quickly shifting target. To keep your company ahead of the game, we provide three big-picture tips for covered businesses in anticipation of the fast-changing state privacy landscape in 2023:

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Telecom, Media & Technology

1. Pay Attention to the Rulemaking Activity in California and Colorado—the New Rules Will Likely Impose New Expectations on Impacted Businesses.

Of the five new state laws that will come into effect this year, two authorize rulemakings: California and Colorado. In California, the new privacy agency—the California Privacy Protection Agency (CPPA)—is charged with developing new rules to implement the CPRA. In Colorado, the Attorney General (AG) is developing rules to implement the CPA.

In both states, the draft rules are broad and would impose new and specific requirements on covered organizations beyond those contemplated by the respective statutes. For example, both state rulemakings are tackling issues related to automated decision-making, data privacy impact or risk assessments, and consumer consent, among other significant issues that will affect business operations. Covered businesses should monitor these rulemaking proceedings and be prepared to update their compliance strategies once the rules are finalized.

- In California, although the new law took effect January 1, 2023, the implementing rules are still in flux. So far, the CPPA is conducting two rulemaking proceedings under the CPRA. The first rulemaking proceeding—which covers several aspects of the law, including required notices, consent, and responding to consumer requests, among other things—is well underway. The agency has released several drafts of the first set of rules and has sought public feedback. Based on statements from the CPPA, companies should expect these rules to be final in the first half of 2023. Once the first set of rules is finalized, the CPPA will launch a second rulemaking, which will cover automated decision-making, risk assessments, and cybersecurity audits.
- In Colorado, the AG has released two drafts of the proposed CPA rules and has a formal rulemaking hearing scheduled for February 1, 2023. The window for filing written comments in response to the proposed rules is still open: while the comment deadline technically closes on February 1, 2023, the deadline to have any proposed revisions presented at the formal rulemaking hearing is January 18, 2023

2. Keep an Eye on Enforcement Activity in All of the States to Better Understand How these New and Complex Requirements Are Interpreted by Their Respective Enforcement Agencies.

Each of the five new privacy laws have enforcement regimes that are unique to their respective states. For example, in California, when civil and administrative enforcement of the new CPRA provisions begins in July, it will be divided between the AG and the new CPPA; additionally, there is a limited private right of action in the case of security breaches. Accordingly, covered businesses should monitor enforcement developments from the AG, the CPPA, and private litigation (in the case of security breaches) to understand how the law is being applied and interpreted.

While the enforcement actors and frameworks vary from state to state, the same principle holds true across all five states: covered businesses should closely monitor enforcement activity to understand trends and expectations, especially given how complex and technical these new laws are.

3. Do Not Reinvent the Wheel—Where Possible, Develop Privacy Programs that Can Broadly Satisfy Common Requirements Across the Various State Laws.

Finally, companies that are subject to multiple new state privacy laws should work to develop "global" privacy programs that can comply with multiple frameworks, where feasible. At a high level, this approach is more workable where the new state laws have consistent or overlapping expectations, such as similar data minimization and data security requirements or the same consumer rights. For example, companies that have already gone through the process of conducting data privacy assessments under the VCDPA should be able to leverage those assessments to comply with new requirements in Colorado and Connecticut later this year.

With that said, there will of course be outlier obligations in the various states that need to be factored into compliance programs—for example, the unique and prescriptive website link requirements under the California framework. Organizations that are subject to multiple state laws should aim to develop compliance programs that are broad enough to satisfy current applicable privacy laws and regulations while taking account of unique requirements.

***

Wiley's Privacy, Cyber & Data Governance Team has helped entities of all sizes from various sectors proactively address risks and address compliance with new privacy laws. Join our upcoming webinar on January 12, 2023—**Staying Ahead of State Privacy Laws: Tips and Best Practices for Building Compliant Strategies for Five Key States**—where we will review best practices for developing compliant strategies across all five states and discuss ongoing regulatory activity in California and Colorado, flagging key privacy and security issues to watch and how new rules may impact your organization's compliance plan.