

October 2022

Client Advisory

Privacy Law Changes Are Coming: Is Your Business Ready?

Consumers are doing more business online than ever. Everyday online transactions, such as ordering take out, ride sharing, and subscribing to content subscription services present unlimited opportunities for bad actors to gain unauthorized access to consumers' personal information. Accordingly, consumers need and expect expanded privacy protection to protect their information processed in connection with such everyday transactions.

As a result of this shift, many US states, including California, Virginia, Colorado, and Connecticut have passed comprehensive privacy regulations aimed to protect their residents' personal information or personal data. Close to 30 other states, including New Jersey, have drafted similar legislation for debate. Importantly, these comprehensive state privacy laws are not limited to companies organized or physically located in such states. They have extraterritorial application based upon unique threshold requirements. As a result, US companies are now subject to an evolving patchwork of state and industry-specific privacy laws with different, and in some cases, conflicting requirements.

California Leads the Charge Among US States to Implement Comprehensive, Consumer-Friendly Privacy Regulations

On January 1, 2020, the California Consumer Privacy Act (CCPA) went into effect, giving California residents greater rights over their personal information, including: (1) the right to know what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold; (2) the right to "opt out" of allowing a business to sell their personal information to third parties; (3) the right to have a business delete their personal information, with some exceptions; and (4) the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the CCPA.

On November 3, 2020, California amended the CCPA by passing the California Privacy Rights Act (CPRA), which expands the rights granted to California consumers under the CCPA and introduces some new

privacy rights. Like the CCPA, the CPRA applies not only to businesses located in California, but to for-profit businesses located anywhere that do business in California and collect personal information from California consumers, and meet one of the following threshold criteria:

1. the business had over \$25 million in gross revenue in the preceding calendar year; or
2. the business buys, sells, or shares the personal information of 100,000 or more consumers or households; or
3. the business derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

The CPRA also applies to any entity that controls or is controlled by a business that meets these criteria and that shares consumers' personal information.

Under the CPRA, businesses are also subject to new requirements related to data retention, data minimization, and purpose limitation, and they must flow such obligations down to contractors and third parties to which the businesses have sold or shared information.

Enforcement will be tougher under the CPRA, which lacks the mandatory 30-day cure period provided under the CCPA, and triples penalties for violations involving minors under the age of 16. The California Privacy Protection Agency will begin enforcing the CPRA beginning on July 1, 2023.

If your company does business in California and has an annual revenue of over \$25 million dollars, or derives the majority of its profits from selling personal information, you are likely subject to CPRA and should begin working towards compliance.

Virginia, Colorado, and Connecticut Follow California's Lead

Virginia, Colorado, and Connecticut followed California's lead when they passed their respective comprehensive state privacy laws, including the Virginia Consumer

Data Protection Act (VCDPA), which becomes effective on January 1, 2023, the Colorado Privacy Act (CPA), which becomes effective July 1, 2023, and the Connecticut Data Privacy Act (CTDPA), which becomes effective July 1, 2023.

regarding a specific issue or problem. Advice should be obtained from a qualified attorney or tax practitioner licensed to practice in the jurisdiction where that advice is sought.

Like the CPRA, these new state privacy laws can apply to businesses that do not have a physical presence in such states. Similar to the CPRA, the VCDPA, CPA and CTDPA provide consumers with certain rights related to their personal data, such as the right to know what data a business has collected about them, the right to delete or correct personal data, and the right to opt out of the processing of personal data for targeted advertising purposes, among others. Some businesses subject to one or more of the new state privacy laws will be required to conduct and document data protection assessments for processing activities involving personal data, which includes weighing the potential risks of processing personal data against the direct or indirect benefits of processing to the controller, consumer, and the public.

Additionally, businesses subject to such laws must provide consumers with a privacy policy that details the categories of personal data processed, the purpose for the processing, how consumers may exercise their rights and appeal the controller's decision regarding consumer requests, categories of personal data that the controller shares with third parties, and the categories of third parties with whom the data controller shares personal data. While the VCDPA, CPA, and CTDPA share many similar requirements, there are important distinctions among them, including the threshold requirements for application.

Conclusion

In light of the privacy law changes coming in 2023, companies doing business in California, Virginia, Colorado and/or Connecticut should assess their data privacy compliance and consider updating their privacy policies and vendor agreements, implementing data subject request procedures, and adopting additional security measures and training, if necessary. For assistance in assessing whether your business is covered by the CPRA, VCDPA, CPA, or CTDPA, and working toward compliance, please reach out to Kate Sherlock at 856-673-3919 or ksherlock@archerlaw.com.

DISCLAIMER: This client advisory is for general information purposes only. It does not constitute legal or tax advice, and may not be used and relied upon as a substitute for legal or tax advice