HUDSON COOK

2023 to Bring Major Changes to Consumer Data Privacy Regulation

November 30, 2022 | Webb McArthur

One month remains for businesses to prepare for significant chances to consumer data privacy laws in the US. The nation's first comprehensive consumer data privacy law, the California Consumer Privacy Act (CCPA), is set to undergo significant updates on January 1. Regulations are still being updated, so compliance efforts will continue into the new year. Additionally, the second comprehensive state law, in Virginia, will be effective and enforceable. The law is similar to the CCPA, but not identical, and impacted businesses will need to separately consider compliance with both laws. While these laws contain exemptions for financial services providers, all businesses directly subject to the laws will need to ensure that their data is inventoried to consider the impact on data sets like website data, marketing data, and data on employees.

First, major changes are coming to the CCPA by way of the California Privacy Rights Act (CPRA), a 2020 ballot initiative. California residents will have new rights with regard to their personal information, including the right to opt out of the sharing of their personal information for cross-contextual advertising, the right to limit the use and disclosure of sensitive personal information (a new subset of personal information), and the right to correct their personal information. The CPRA also adds new notice content requirements, requires businesses to pass on deletion requests to third parties to which they have transferred personal information, and imposes data security requirements. Further, the law adds new requirements when managing service providers and will require contracts to transfer (or "sell") personal information to third parties. In implementing new requirements, business will need to take particular care to consider the impact of the law on information passively collected or processed by a website or identified with regard to a device, a focus of the regulator.

The CCPA's limited exemptions related to employment and B2B context information are also expiring. With this development, California-resident employees and other individuals acting in commercial contexts will now have CCPA rights, and business will have to amend disclosures to cover this information. Otherwise, the CCPA's exemptions remain intact.

The California Privacy Protection Agency, the new entity that has taken over rulemaking under the CCPA from the Attorney General, is working on updating the CCPA regulations. These regulations, when finalized, will impact notice content, the rules surrounding processing of consumer requests, and the circumstances under which businesses may process personal information secondary to the purposes for which it was collected. Businesses should monitor CPPA rulemaking efforts, as rules related to profiling opt outs and managing online opt-out signals are anticipated.

In addition to big changes to the CCPA, Virginia's new data law also becomes effective on January 1.

That law, the Virginia Consumer Data Privacy Act (VCDPA), applies to businesses that control or process personal data on at least 100,000 Virginia residents in a year, or that control or process personal data on at least 25,000 Virginia residents in a year where they derive over 50% of their gross revenue from the sale of personal data. The law comes with similar (but not identical) exemptions to the CCPA. One distinction to note for Virginia is that, in contract to the CCPA, the VCDPA exempts not only personal *data* subject to the Gramm-Leach-Bliley Act (GLBA) but also "*financial institutions*" as defined by the GLBA. Additionally, unlike the CCPA, the VCDPA does not apply to personal data in employment or commercial contexts.

The VCDPA comes with many of the same consumer rights and business requirements as the CCPA, but with a few new and different obligations to note:

- Consumers in Virginia will have the right to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. Here, "profiling" means the automated processing of personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

- Businesses will have to obtain opt-in consent to process sensitive personal information, not just extend an opt-out right.

- Consumers will have the right to appeal denials of consumer rights.

- Businesses will have to conduct and document data protection assessments when engaging in certain data activities, like selling data, processing personal data for targeted advertising, engaging in profiling, or any other activity that presents a heightened risk of harm to consumers. These assessments are required to identify and weigh benefits and risks—to the business, the consumer, other stakeholders, and the public—related to the proposed data processing activity, as well as whether risks may be appropriately mitigated by safeguards. Assessments must be written and may be demanded by the Virginia Attorney General as related to an investigation.

Consumer data privacy compliance will continue to be an ongoing effort in 2023, as the consumer data privacy landscape continues to evolve through new laws and regulations. Laws in Colorado, Connecticut, and Utah are set to take effect later in 2023, and Colorado is currently engaged in rulemaking efforts related to its law. More states will consider next year broad privacy legislation, as well as more targeted proposals, like those related to biometric information, geolocation information, and website information. The FTC is considering broad privacy and data security rulemaking, the CFPB is working on implementing consumer rights to personal financial records under section 1033 of the Dodd-Frank Act, and debate about federal privacy legislation will likely start back up in the new Congress. Amidst the changing landscape, businesses are strongly encouraged to keep data inventory and mapping efforts up to date and consider the risks—in addition to the opportunities—that come out of data collection and processing.

HUDSON
COOK

Hudson Cook, LLP is a national law firm representing the financial services industry in compliance, privacy, litigation, regulatory and enforcement matters.

7037 Ridge Road, Suite 300, Hanover, Maryland 21076
410.684.3200

hudsoncook.com