June 22, 2023

Need Help Navigating the Alphabet Soup of State Consumer Privacy Laws?

CCPA, CPA, CTDPA, VCDPA, UCPA, ICDPA, INCDPA, TIPA, MTCDPA … how does one even begin building a compliance program that addresses this alphabet soup of state consumer privacy laws? The thought of having to comply with this patchwork of similar yet slightly different state consumer privacy laws may be daunting for the compliance team at any organization, particularly as the lists of enacted and proposed state consumer privacy laws continue to grow at a rapid rate. Day Pitney privacy lawyers are actively monitoring the ever-changing state privacy landscape and developing compliance programs for our clients.

The Current Landscape

Last year, businesses were gearing up for the five state privacy laws that took or are set to take effect this year:

- California: California Consumer Privacy Act (CCPA), amended by the California Privacy Rights Act (CPRA), effective January 1
- Colorado: Colorado Privacy Act (CPA), effective July 1
- Connecticut: Connecticut Data Privacy Act (CTDPA), effective July 1
- Utah: Utah Consumer Privacy Act (UCPA), effective December 31
- Virginia: Virginia Consumer Data Protection Act (VCDPA), effective January 1

State legislators continue to pass state consumer privacy laws, so, at the time of writing, the list has recently grown to include Iowa, Indiana, Tennessee and Montana. Iowa's privacy law, the Iowa Consumer Data Protection Act (ICDPA), takes effect January 1, 2025. The ICDPA applies, with certain specified exceptions, to a person conducting business in Iowa or producing products or services targeted to Iowa consumers who does either of the following in a calendar year: (1) controls or processes the personal data of at least 100,000 Iowa residents or (2) controls or processes the personal data of at least 25,000 Iowa residents and derives more than 50 percent of their gross revenue from the sale of personal data. The ICDPA contains a framework similar to that of its predecessors, providing consumers with the following rights: (1) to confirm whether a business is processing their personal data and to access such data; (2) to obtain a copy of their personal data; (3) to request deletion of their personal data maintained by the business; and (4) to opt out of the sale of their personal data. However, the ICDPA contains some notable differences from other states' laws, including not providing consumers with the right to correct inaccuracies in their personal data. Indiana's privacy law, the Indiana Consumer Data Protection Act (INCDPA), takes effect January 1, 2026, and it substantially overlaps with the other enacted state privacy laws. Similar to the ICDPA, the scope of the INCDPA encompasses persons who conduct business in Indiana or produce products or services that are targeted to Indiana residents and that during a calendar year do either of the following: (1) control or process the personal data of at least 100,000 Indiana residents or (2) control or process the personal data of at least 25,000 Indiana residents and derive more than 50 percent of their gross revenue from the sale of personal data. Of note, similar to the Colorado, Connecticut, Tennessee, Virginia and Montana laws, the INCDPA requires consumer consent to process sensitive data. Tennessee's privacy law, the Tennessee Information Protection Act (TIPA), takes effect July 1, 2024, and its scope of application follows that of Iowa and Indiana. Specifically, the TIPA applies to persons who conduct business in Tennessee or produce products or services that are targeted to Tennessee residents and that during a calendar year do either of the

following: (1) control or process the personal data of at least 100,000 Tennessee residents or (2) control or process the personal data of at least 25,000 Tennessee residents and derive more than 50 percent of their gross revenue from the sale of personal data. Like the laws in Colorado, Connecticut and Montana, the TIPA provides a 60-day cure period for alleged violations, whereby the attorney general will not initiate an action against the business if the business cures the noticed violation of the TIPA within this time. Notably, other than California's, the other state laws also provide for cure periods of varying lengths for alleged violations. In California, the CPRA eliminated the 30-day cure period permitted under the CCPA; however, the law does permit the California Privacy Protection Agency to decide not to investigate a complaint or to provide a business with a time period to cure the alleged violation, considering the business's lack of intent to violate the law and any voluntary efforts undertaken by the business to cure the alleged violation prior to notification of the complaint. Montana's privacy law, the Montana Consumer Data Privacy Act (MTCDPA), takes effect October 1, 2024. The MTCDPA has the lowest threshold for application to businesses of all the state consumer privacy laws. Specifically, the MTCDPA applies to persons who conduct business in Montana or persons who produce products or services targeted to Montana residents and (1) control or process the personal data of at least 50,000 Montana residents, excluding personal data processed solely for the purpose of completing a payment transaction, or (2) control or process the personal data of at least 25,000 Montana residents and derive more than 25 percent of gross revenue from the sale of personal data. Of note, although the MTCDPA provides businesses the right to cure alleged violations within 60 days, this right to cure sunsets April 1, 2026, at which point the Montana attorney general will not have to provide notice to the business of an alleged violation and can pursue enforcement even if the business corrects such violation.

A Road Map for Businesses

In order to prepare for these state consumer privacy laws, businesses should consider taking the following steps:

- Mapping out how and when personal information is collected from consumers
- Gathering information and reviewing relevant contracts regarding:
    - The categories of consumer personal information collected, used, shared with third parties and sold by the business
    - The purpose of such collection, use, sharing and sale of consumer personal information
- Working with counsel to:
    - Determine what state consumer privacy laws apply to the business
    - Draft the privacy notices required under the relevant state consumer privacy laws
    - Draft the forms, policies and procedures regarding the exercise of the rights granted to consumers under the relevant state consumer privacy laws

Day Pitney privacy lawyers are actively working with in-house counsel and business leaders on evaluating the application of these state consumer privacy laws and developing compliance programs. As noted above, coming into compliance with these state laws will require many businesses to take significant steps. We are also continuing to monitor the status of many other pending state consumer privacy laws.

Authors

Stephanie M. Gomes-Ganhão

Associate

Hartford, CT | (860) 275-0193

sgomesganhao@daypitney.com

William J. Roberts

Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com

Kritika Bharadwaj

Partner

New York, NY | (212) 297-2477

kbharadwaj@daypitney.com

Richard D. Harris
Of Counsel

Hartford, CT | (860) 275-0294

New Haven, CT | (203) 752-5094

rdharris@daypitney.com

Mindy S. Tompkins
Partner

Hartford, CT | (860) 275-0139

mtompkins@daypitney.com

John F. Kaschak
Associate

Parsippany, NJ | (973) 966-8034

jkaschak@daypitney.com

Phoebe A. Roth
Senior Associate

New Haven, CT | (203) 752-5045

proth@daypitney.com