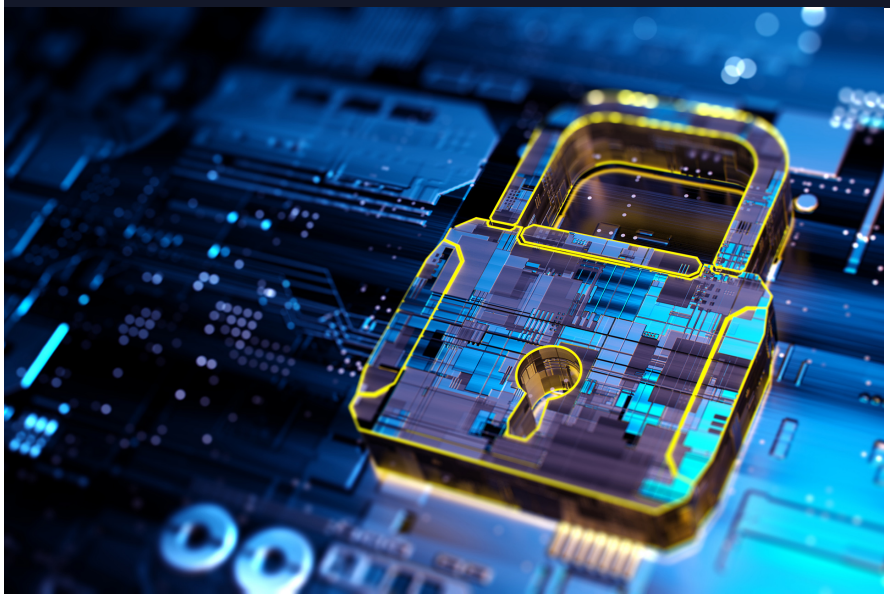
BARNES & THORNBURG LLP



ALERTS

July Brings Enforcement – And Delay – Of New Privacy Laws

July 7, 2023

Highlights

New data privacy laws in Colorado and Connecticut became enforceable July 1

The California's Consumer Privacy Rights Act regulations, originally set to become enforceable July 1, has been delayed until March 2024

Businesses subject to the laws will need to review and possibly update their policies and procedures to ensure compliance

Businesses collecting consumer information in Colorado and Connecticut will need to ensure their privacy practices are compliant this summer, as new state privacy laws became enforceable July 1.

California's amendment to the original California Consumer Privacy Act (CCPA), the California Privacy Rights Act, and its regulations (CPRA), originally shared Colorado and Connecticut's July 1 enforcement date, but a court ruling issued a delay in enforcement of the regulations just days before the original deadline.

The Colorado Privacy Act (CPA) and the Connecticut Data Privacy Act

RELATED PEOPLE

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

Maddie San Jose
Associate
Indianapolis

P 317-231-6416
F 317-231-7433
msanjose@btlaw.com

RELATED PRACTICE AREAS

Data Analytics
Data Security and Privacy
Intellectual Property

(CTDPA) apply to entities or individuals who collect and process the personal data of residents of those two states, subject to applicability thresholds. Although there are several similar aspects and obligations between the laws, certain differences and unique provisions will require businesses to take a second look at their current privacy compliance programs.

Scope and Compliance

When assessing compliance obligations, businesses must determine if they are subject to the new laws based on threshold applicability requirements.

The CPA applies to entities who conduct business in Colorado or sell goods or services to Colorado residents. Businesses meet the threshold when they manage or process the data of 100,000 Colorado consumers yearly, or derives revenue from selling personal information while also controlling the personal data of at least 25,000 Colorado residents.

The CTDPA applies to both businesses operating in Connecticut and those that maintain or provide services involving personal data for businesses operating in Connecticut. The threshold limits for the CTDPA are similar to Colorado, but also require that at least 25 percent of the controller's gross revenue comes from the sale of personal information when collecting the personal data of 25,000 Connecticut residents.

Both exempt different types of entities and data depending on certain circumstances, including government agencies and data covered under federal privacy laws.

Ensuring Compliance With the New Laws

Businesses already compliant with the Virginia Consumer Data Protection Act (VCDPA) and California's law will find they are mainly compliant with Colorado and Connecticut, aside from a few distinct provisions. However, businesses not currently subject to the VCDPA may be subject to the CPA and CTDPA, and should ensure they are prepared for compliance.

For example, the CPA and CTDPA expand the definition of the "sale" of personal data. The VCDPA defines sale of personal data as exchanging data for monetary value only. On the other hand, CPA and CTDPA define sale as exchanging data for money or any other valuable consideration, similar to the California law.

In addition, like the Virginia law, sensitive personal data has its own category in Colorado and Connecticut. All three acts require consent from consumers before processing sensitive personal data.

The CPA and CTDPA both contain lenient cure periods of 60 days, a drastic expansion compared to Virginia and California. However, on Jan. 1, 2025, the cure periods for the CPA and CTDPA will sunset and no longer be available to businesses out of compliance.

Delayed Enforcement of the CPRA Regulations

The CPRA, which took effect on Jan. 1, 2023, was set to become enforceable just six months after enactment. However, on June 30, a

Sacramento County Superior Court issued an emergency ruling that stated the July 1 enforcement date of the regulations was too soon after the amendment's passing, due to the California Privacy Protection Agency's (CPPA) delay in publishing them.

The June 30 ruling gives California businesses six additional months to become complaint with the regulations, which will now become enforceable on March 29, 2024. However, the body text of the statute of the CPRA remains fully enforceable. As one of the strictest privacy laws in the United States, the CPRA eliminated the cure period for businesses. After enforcement, businesses that are found to violate the CPRA will be subject to immediate fines.

Despite this extension, businesses subject to the California law should act now to ensure compliance with the regulations, as the new law adds several new requirements for businesses, and additional consumer rights.

Compliance Checklist

In preparation for enforcement of the new laws, companies should determine whether they currently meet the applicability thresholds that would require them to comply.

Other best practices companies should consider include:

- Assessing the collection, use, and processing of personal information, which could include performing a data audit and gap analysis to the requirements of the applicable laws
- Reviewing website privacy policies and terms of use for transparency and proper notice to individuals about the processing of personal information
- Assessing whether internal information management policies and/or procedures may need to be revised and whether additional procedures are necessary
- Reviewing insurance policies (particularly, but not limited to, cybersecurity coverage) closely to see whether and how liabilities under the new laws would be covered
- Ensuring company websites are equipped to recognize and respond to Global Privacy Control signals and that they display the legally required links and forms, a new legal requirement under the new laws
- Reviewing third-party agreements to ensure compliance with the newly enforceable laws
- Establishing or updating data subject access request procedures and data retention policies to minimize liability

For more information, please contact the Barnes & Thornburg attorney with whom you work or Brian McGinnis at 317-231-6437 or brian.mcginnis@btlaw.com or Maddie San Jose at 317-231-6416 or msanjose@btlaw.com. This alert was drafted with the assistance of Jimmy Magee, summer associate.