CLIENT ALERTS & INSIGHTS

REMINDER: One Month Until Colorado and Connecticut Data Protection Laws take Effect; California Enforcement Poised to Begin.

JUNE 1, 2023

Enacted in 2022, the laws in Colorado and Connecticut will now join California's and Virginia's laws in placing broad obligations and requirements on businesses' data collection and use practices.

This year has seen a flurry of new data protection laws and regulations-especially at the state level. That will continue this summer as Colorado and Connecticut's data protection laws come into effect on July 1 and enforcement begins for California's updated law-also on July 1.

The California Privacy Rights Act-which amended the California Consumer Privacy Act-has been in effect since January 1, 2023. There are even more states with broad data protection laws coming into effect over the course of the coming years.

California and Virginia's data protection laws are already in effect, with California delaying enforcement until July 2023. Colorado, Connecticut, and Utah's data protection laws will come into effect over the course of 2023 as more and more businesses in the U.S. becomes subject to one or more data protection laws. Iowa more recently passed their data protection law last month and it will go into effect January 1, 2025.

Indiana's data protection law provides a long runway for in-scope entities to come into compliance as the effective date of the Indiana Law is January 1, 2026.

Despite more recent passage through their applicable state legislatures, the Montana's data protection law and Tennessee's data protection law come into effect **before** some already existing data protection laws. The Montana's is effective as of October 1, 2024, and the Tennessee's is effective July 1, 2024.

Prior to 2021, California was the only U.S. state with a comprehensive data protection law. Now, there are 9 and 2023 will likely continue to see more states enter the data protection foray so as not to be left behind from the wave of data protection legislation.

Colorado and Connecticut Data Protection Law Privacy Rights

Under the Colorado and Connecticut data protection laws, consumers have the following rights:

- to confirm whether a business is processing the consumer's personal information,
- to correct the personal information a business holds about them;
- to have their personal information deleted;

- to receive a copy of the personal information held about them in a portable and usable form (data portability);
- to opt-out of the sale of their personal information;
- to opt-out of cross-contextual behavioral targeted advertising; and
- to opt-out of profiling through solely automated means in furtherance of decisions with legal or similar effect (e.g., employment, education, criminal justice, etc.);

Additionally, where a business sells personal information, individuals have the right to obtain a specific disclosure of (i) the categories of personal information sold about the individual; (ii) categories of third parties which the information was sold to (by category of personal information sold); and (iii) the categories of their personal information disclosed for a business purpose.

The laws define "sale" as the exchange of personal information for monetary **or other** purposes-which aligns with California's broad approach to sale including more than data brokers.

Similar to other recent state data protection laws, the laws require businesses to allow individuals the ability to appeal any denial of their exercise of any data privacy request.

Instead of merely requiring the provision of a right opt-out-such is the case under the California and Utah data protection laws-the Colorado and Connecticut laws require businesses to obtain prior opt-in consent before processing an individual's sensitive personal information. "Sensitive personal information" includes, for example: (1) race, ethnicity, or religion; (2) mental or physical health diagnosis; (3) sexual orientation; (4) citizenship or immigration status; (5) genetic or biometric data processed with the purpose of identifying an individual; (6) the personal information of a child (younger than 13); or (7) a person's precise geolocation (within a radius of 1,750 feet).

Colorado Universal Opt-Out Mechanism

Where businesses are engaging in activity related to Colorado consumers' personal information that are considered to be a "sale" or "cross-contextual behavioral" advertising, those businesses must also implement universal opt-out mechanisms that allow consumers to opt-out of both types of activities.

Under the applicable regulations and beginning on July 1, 2024-one year after the Colorado law's effective date-all in-scope business will need to (i) configure all of their websites to recognize any universal opt-out mechanisms (as identified by the Colorado Department of Law); (ii) treat all signals received from universal opt-out mechanisms as a valid request by an individual to opt-out of targeted advertising and/or the sale of their personal information (as applicable); and (iii) continue treating the individual as having opted-out until the individual opts-in to targeted advertising or sale of their personal information.

No later than January 1, 2024, the Colorado Department of Law will announce an initial list of universal opt-out mechanisms that businesses will need to accept as valid opt-out requests. However, the Colorado regulations set forth technical specifications that any universal opt-out mechanism must meet in order to be recognized.

The mechanism must (i) allow for the automatic communication of their opt-out choice to multiple businesses (e.g., through commonly used coding formats such as HTTP or JavaScript); (ii) allow for the individual to clearly communicate their opt-out rights; (iii) store, process, and transmit the information necessary for the business to effectuate the opt-out request; (iv) must have in place reasonable security measures for the transmission of such information; and (v) must not unfairly disadvantage the business (e.g., anti-competitive practices) or prevent the business's ability to verify the request or determine whether the individual is a resident of Colorado.

Additionally, it is important to note that a universal opt-out mechanism cannot be a default setting. Meaning, the opt-out options cannot come pre-installed or pre-configured on a device, browser, or operating system. The opt-out setting still needs to be made by the individual's affirmative choice. This does not preclude an individual from exercising an opt-out right through the use of a browser add-on / plug-in, however.

It is important to note that a business can-after receiving a universal opt-out signal from an individual-enable that individual to later consent to targeted advertising or the sale of their personal information.

Therefore, for individuals who have enabled universal opt-out mechanisms, a business can present individuals with a link to opt-in to targeted advertising or the sale of their personal information, instead of merely providing an opt-out link.

This is a huge departure from previous US state laws that instead relied on individual, specific opt-out rights in order to give individuals more control over their information. Colorado's universal opt-out requirements flips that legal regime on its head as a business will now be required to obtain prior consent from those individuals with universal opt-out mechanisms implemented.

Colorado and Connecticut Data Protection Assessments

The data protection laws in Colorado and Connecticut require businesses conduct data protection assessments and offer guidance on when exactly assessments and audits are required.

If a business is under any of these two states' data protection laws, they are prohibited from processing personal information in a manner that presents a higher risk of harm to the individual consumer without first conducing and documenting a data protection assessment. High risk processing includes: (1) targeted advertising or profiling that presents a reasonably foreseeable risk of (a) financial harm, (b) unfair or deceptive treatment, (c) intrusion on the solitude or seclusion of private affairs (based on a "reasonable person" standard), or (d) other substantial injury to the consumer; (2) the sale of personal data; or (3) any processing that involves sensitive personal information.

If a data protection assessment is required, it must identify and weigh the benefits of the processing against the potential risks-specifically the risks to the individual rights a consumer has over their personal information. Any such assessment should also factor in the existence or possibility of safeguards that mitigate the risks.

These would include heightened encryption standards, anonymization and/or aggregation of the information, access control measures, etc. In fact, the assessment needs to specifically weigh the

use of de-identified information and what the consumer's reasonable expectations are based on their relationship to the in-scope business.

Finally, in both states, the data protection assessments must be made available to the applicable state's attorney general as they may request.

It is important to note that separate assessments covering individual processing activities are not necessary. A single data protection assessment can be used to cover multiple processing activities so long as the processing and information involved is sufficiently similar.

Colorado, Virginia, and Connecticut Processors

Colorado's and Connecticut's new data protection regimes set forth a simpler third party dynamic. Under these new U.S. state data protection laws, parties are either considered a "controller" or a "processor". A party is a controller if they-alone or in joint decisions with others-determine the purposes for and means of processing personal information. A party is a processor if they are processing the personal information on behalf of the controller.

Like California, a contract is required in all cases when personal information is shared or accessible to a third party.

To effectuate a controller - processor relationship, the controller and processor must enter into a binding contract that delineates the parties' respective responsibilities and the processing instructions the processor must adhere to. The contract between the two parties must contemplate and provide that (1) each person involved in processing is subject to a duty of confidentiality with respect to the personal data; (2) at the controllers direction and option, for the processor to delete or return personal data to the controller (unless prohibited by applicable law); (3) audit and review obligations that allow the controller to ensure the processor is complying with the applicable law; and (4) only engage subcontractors pursuant to written contracts that set forth the same or heightened obligations on the subcontractor; and (5) only disclose the information to subcontractors after giving the controller a reasonable opportunity to object to the engagement of such subcontractor.

Practically-and in line with the requirements set forth in California-controllers will likely need to set up express requirements around notifications for and compliance with data subject right requests.

Data Protection Law Enforcement

Neither the Colorado nor the Connecticut data protection law provide individuals with a private right of action against businesses that violate the legal requirements.

Instead of a private right of action, the state's respective Attorney Generals will have exclusive enforcement authority.

Prior to any enforcement action, the state Attorney General is required to provide the business a 60 day notice allowing the business 60 days to cure the alleged violation. It is only if the alleged violation is not cured within such 60 day period that the state Attorney General can bring an enforcement action.

Colorado's cure right sunsets on January 1, 2025 and the Connecticut cure right sunsets December 31, 2024.

Effective Dates



Scope and Applicability of U.S. State Data Protection Laws

All states set forth a prerequisite that only a business that operates or does business in the specific state is subject to the law. But it is not that simple. To be subject to the applicable state laws, the "do business in the state" prerequisite must be met, but a business must also meet certain "triggers".

There are generally three triggers that could bring a business into the scope of a U.S. State's data protection law: (1) annual gross revenue (not just the revenue derived out of the applicable state); (2) the total collection of personal information from consumers in the applicable state; or (3) the collection and sale of the state's consumers' personal information.

State	Annual Gross Revenue (Aggregate / Worldwide)	Processing of Personal Information (Applicable State Residents)	Sale of Personal Information Residents)
California	OVER $25 million	Buying, selling, or sharing 100,000 or more consumers' personal information	50% of gross revenue (aggreg consumer personal informatic
Colorado	N/A	Processing 100,000 or more consumers' personal information	Receiving **any** profit from the personal information and con processing at least 25,000 cor information
Virginia	N/A	Processing 100,000 or more consumers' personal information	Deriving 50% of annual gross from selling personal informa or processing at least 25,000 personal information
Connecticut	N/A	Processed 100,000 or more consumer' personal information	Deriving 25% of annual gross from selling personal informa or processing at least 25,000 personal information
Utah	**REQUIREMENT:** $25 million or more	Processing 100,000 or more consumers' personal information	Deriving 50% of annual gross from selling personal informa or processing at least 25,000 personal information
Iowa	N/A	Processing 100,000 or more consumers' personal information	Deriving 50% of annual gross from selling personal informa or processing at least 25,000 personal information
Indiana	N/A	Processing 100,000 or more consumers' personal information	Deriving 50% of annual gross from selling personal informa or processing at least 25,000

As the above table indicates, each state has taken a slightly different approach. California arguably has the broadest reach in that **any** business that records an annual gross revenue of over $25 million is subject to the CPRA. Although Montana's lower threshold of processing 50,000 consumers' personal information (in contrast to the 100,000 threshold most states have adopted) might have a broad reach as well.

It is also important to note a big difference between California and the other 8 U.S. states-California includes employee, job applicant, contractor, and business-to-business personal information in the scope of the law. The other 8 U.S. states all include broad exclusions that exempt out the forgoing employee and business-to-business personal information categories.

Utah is still arguably the narrowest in scope in that on top of the "do business in the state" threshold requirement, Utah also requires a prerequisite that the business have an annual gross revenue of $25 million or more. Then, assuming the first two prerequisites are met, a business must meet one of the two collection or sale of personal information triggers.

Conclusion

In 2022, the federal government again failed to seriously consider an omnibus data protection law that would preempt the increasing number of state data protection laws; and it is unlikely the federal government will implement such a federal law anytime soon.

Meanwhile, states will continue to enter the fray of comprehensive data protection laws. While those laws will undoubtably cover similar concepts-they will all present different and important nuances that will require detailed reviews of data protection compliance programs. This has proved true in 2021 and 2022 with California, Colorado, Connecticut, Utah, and Virginia; and now in 2023 with Iowa, Indiana, Montana, and Tennessee.

As more states pass comprehensive data protection laws and such laws come into effect, more and more business will need to build out substantive, data protection compliance programs.

Those programs will need to adaptable-as one business could be subject to multiple state laws and therefore must adapt to the nuanced differences-and will need to account for the different aspects of comprehensive data protection laws, such as (1) substantive privacy policies and notices; (2) consumer privacy right request policies and procedures; (3) reasonable, adequate technical, organizational, and physical security measures; (4) vendor and contract management programs to flow through required contractual provisions when engaging data processors and service providers; and (5) regular audit procedures and programs.

The above list is not exhaustive of all a business would need to do under the applicable U.S. State laws; but it provides an example of the different requirements comprehensive data protection laws set forth-and the time it will take for business to build out compliant programs.

Businesses that have not previously dealt with comprehensive data protection law compliance will need to invest a significant amount of time in developing the required policies and procedures. Additionally, even if businesses have previously dealt with other-or former versions of-comprehensive data protection laws, they will need to conduct comprehensive reviews to account for specific nuances and difference in the laws.

As more states continue to implement their own variations of data protection laws and business juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.