LEGAL UPDATES

CCPA, VCDPA, CPA, and CTDPA … Oh my!

The privacy landscape is changing, again, and your company should ensure compliance with the new privacy laws. Here's what you need to know.

10/03/2022 | 6 minute read

The privacy landscape is changing, again, and your company should ensure compliance with the new privacy laws. On January 1, 2023, the California Privacy Rights Act (CPRA) and the Virginia Consumer Data Protection Act (VCDPA) will become operative. And, shortly thereafter – on July 1, 2023, the Colorado Privacy Act (CPA) and the Connecticut Data Privacy Act (CTDPA) will become operative – with the Utah Consumer Privacy Act (UCPA) not too far out either, which becomes operative on December 31, 2023.

Draft rules have been published for CPRA and CPA that provide helpful and clarifying guidance, but such rules will not be released for CTDPA, VCDPA, and UCPA, since the laws currently do not vest rulemaking authority with any agency or office. Although there is some overlap between the laws, compliance with one law does not necessarily mean compliance with rest – even if your business is compliant with the most stringent law. Such non-compliance can result in adverse and expensive, yet avoidable, consequences. We know that these changes can be a source of confusion – maybe even frustration, and Hopkins & Carley is here to guide and support you through the changes.

With the exception of CPRA, the newly enacted privacy laws borrow terminology from the EU's General Data Protection Regulation (GDPR), e.g., controller and processor, so some of these terms may look familiar.

Additionally, like CPRA, CPA and CTDPA prohibit the use of "dark patterns" to obtain consumer consent. If you would like to learn more about "dark patterns," please read our brief publication *Beware of Dark Patterns – What to Watch Out For*.

Below is an overview of the upcoming state privacy laws to consider and address.

California: CPRA

As mentioned above, CPRA becomes operative on January 1, 2023, but has an enforcement start date of July 1, 2023. However, like CCPA, CPRA has a 12-month "look-back" requirement that allows consumers to request their data records dating back a whole year from when the request is made. This means that

Related Services

Data Privacy & Cybersecurity Compliance

Related Sectors

Retail & E-Commerce

organizations must identify collected records of personal information that date back to January 1, 2022.

CPRA is an amendment to the California Consumer Privacy Act (CCPA), which was passed with the intent to clarify parts of CCPA. As such, CPRA adds definitions and provisions to both narrow and expand its scope, depending on the business. Violation of the law is subject to injunction and the business is liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation. And, in limited circumstances, consumers have a private right of action.

Virginia: VCDPA

As mentioned above, VCDPA goes into effect on January 1, 2023, but no enforcement date has been provided. Like other privacy laws, VCDPA adopts a notice, access, choice, and consent approach.

VCDPA applies to persons that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that:

- Control or process personal data of at least 100,000 Virginia consumers annually; or
- Control or process personal data of at least 25,000 Virginia consumers and derive more than 50% of gross revenue from the sale of personal data.

For violations of VCDPA, the state attorney general can seek damages of up to $7,500 for each violation. Notably, VCDPA does not provide for a private right of action.

Colorado: CPA

On September 30, 2022, the Colorado Attorney General's Office published proposed CPA rules, which elaborate on responding to consumer requests, privacy notice requirements, and incentive programs, among other areas. As mentioned above, CPA goes into effect on July 1, 2023.

CPA applies to a controller that conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and

- Controls or processes the personal data of 100,000 Colorado consumers or more during a calendar year; or
- Derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls, the personal data of 25,000 Colorado consumers or more.

Additionally, unlike other state privacy laws, CPA applies to nonprofits that meet the threshold requirements.

CPA contains a 60-day cure period to allow a controller or processor to cure an alleged violation, but this cure period is subject to a sunset provision that is set to expire on January 1, 2025. Violations of CPA that are not cured after the 60-day cure period or after the expiration of the sunset provision are subject to a $20,000 per violation fine.

Connecticut: CTDPA

CTDPA is most similar to CPA with some notable variations. As mentioned above, CTDPA goes into effect on July 1, 2023.

CTDPA applies to persons that conduct business in Connecticut or produce products or services that are targeted to Connecticut residents, and who during the preceding year, either:

- Controlled or processed the personal data of 100,000 or more consumers annually, except for personal data controlled or processed solely for the purpose of completing a payment transaction; or

- Derived over 25 percent of their gross revenue from the sale of personal data and controlled or processed the personal data of 25,000 or more consumers.

Like CPA, CTDPA provides a sunset provision for a 60-day cure period that expires on December 31, 2024. After the expiration of the cure period, the state attorney general may, but is not required, provide an opportunity to correct an alleged violation. Violations of the CTDPA carry civil penalties of up to $5,000 per violation for willful offenses.

Utah: UCPA

UCPA is both similar to and different than, CPRA, VCDPA, and CPA. However, in practice, UCPA is more business-friendly than the other state privacy laws. As noted above, UCPA goes into effect on December 31, 2023.

UCPA applies to a for-profit business that:

- Conducts business in Utah or produces a product or service that is targeted to Utah residents; and
- has annual revenue of $25 million or more; and either:
    - controls or processes personal data of 100,000 or more Utah consumers in a calendar year, or
    - derives over 50% of its gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more Utah consumers.

UCPA provides a 30-day cure period for alleged violations. If the alleged violation is not cured within 30 days, the state attorney general may seek actual damages for the consumer and civil penalties of up to $7,500 per violation.

What should companies do now?

The following short checklist provides a high-level overview of key actions to be taken by entities subject to the CPRA, CPA, CTDPA, VCDPA, and UCPA. Unless otherwise specified, the recommendations apply to all five state privacy laws.

- Data mapping:
    - Map out how personal data and/or sensitive data is collected, used, shared, and deleted – take stock of data flows in and out of the organization. Minimize data that you collect and retain.
- Third Party Assessments and Agreements:
    - Update or implement a data processing agreement or addendum for each vendor that contains specific language for vendors to qualify as processors, and so as not to be considered a "sale."
    - Conduct third party audits on processors who have access to your consumer personal data that present a "heightened risk to consumer." This includes processing sensitive data, selling personal data, and processing personal data for targeted advertising or profiling that presents a reasonably foreseeable risk. (Note: UCPA does not have this requirement.)
- Policies:
    - Review and update online privacy notices and personnel privacy policies to comply with the disclosure requirements of applicable state privacy law – this includes disclosures of consumer requests that are required by applicable state privacy law.

- Prepare internal policies and procedures to ensure that your organization responds to consumer requests for access, portability, correction, or deletion, or information related to the sale of consumer personal data or to opt-out of such sales, as applicable.

- Review customer agreements for consistency and liability cap mechanisms.

- Operationalize Consumer Rights:

  - Consumers have various rights under each state privacy law, including, the right to know, right of access, right to opt-out of targeted advertising, the "sale" or "sharing" of personal data, or profiling in further of decisions that produce legal or similarly significant effects concerning a consumer (e.g., provision or denial of financial, lending, housing, insurance, education, criminal justice, employment, healthcare, or essential goods or services). (Note: UCPA does not include the right to opt out of profiling.) Consumers also have rights to delete data, rights to data portability, to have data corrected and not to be discriminated for exercising any rights. Ensure consent requirements are instituted for sensitive data. (Note: UCPA requires clear notice and an opportunity to opt out, but opt in is not required.)

- Technological Solutions:

  - After analyzing whether a "sale" or "sharing" of data is occurring, implement a "clear and conspicuous link" for consumer right to opt-out of the "sale" or "sharing" of their personal information. While the VCDPA/CTDPA does not prescribe the label of the link, this clear and conspicuous link is similar to the "Do Not Sell or Share My Personal Information" link required by the CCPA/CPRA – businesses under CPRA must also follow Global Privacy Controls. (UCPA does not have this requirement.)

  - For CTDPA/CPA, as of January 1, 2025 and July 1, 2024, respectively, controllers must allow consumers the option to opt out of targeted advertising and the sale of personal data through an "opt-out preference signal," sent with consumer consent via a platform, technology or mechanism.

- Training:

  - Prepare training materials to train all individuals within the organization with respect to applicable privacy laws, particularly personnel who will be responsible for handling consumer personal data inquiries.

- Security

  - Implement CIS Controls or ensure compliance with other vetted industry standards, as well as implement and update internal policies (incident response plan etc.) – at the very least. The level of security must be commensurate with the nature of the personal data and processing activities performed by your organization.

Conclusion

With CPRA and VCDPA taking effect in just a few months, it is still not too late to start assessing your company's data privacy obligations and begin working towards compliance. Lathrop GPM will continue to monitor updates to regulations and developments related to new and existing privacy laws. If you have any questions or concerns whether the new privacy laws apply to your company and what steps to take, please contact us.