LEGAL UPDATES

The New Year brings Two Updated Privacy Laws on Both Coasts of the U.S. to Consider

It is a new year and with that on January 1, 2023, the California Privacy Rights Act (CPRA), an amendment to the California Consumer Privacy Act (collectively, CCPA) and the Virginia Consumer Data Protection Act (VCDPA) went into effect.

01/19/2023 | 5 minute read

It is a new year and with that on January 1, 2023, the California Privacy Rights Act (CPRA), an amendment to the California Consumer Privacy Act (collectively, CCPA) and the Virginia Consumer Data Protection Act (VCDPA) went into effect. Companies that do business in California and/or Virginia should evaluate whether or not they are subject to these laws. If your business is subject to these laws, you should ensure that your business is compliant and has made all necessary changes to your policies and procedures.

Although there is some overlap between the laws, compliance with one law does not necessarily mean compliance with the other– 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 constant changes in privacy laws can be a source of confusion – maybe even frustration, and Hopkins & Carley is here to guide and support you through the changes. Below is a short overview of some aspects of these laws.

California: CCPA

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

The CCPA applies to businesses that:

- have gross annual revenues in excess of $25 Million (relates to the preceding calendar year; or
- annually buy, sell, or share the personal information of 100K or more consumers or households; or
- derive 50% or more of its annual revenue from selling or sharing consumers' personal information.

Related People

Chiara Portner, CIPP/US

Partner

Redwood Shores

650.804.7672

chiara.portner@lathropgpm.com

Related Services

Data Privacy & Cybersecurity Compliance

Labor & Employment

Corporate & Business

Related Sectors

Retail & E-Commerce

Businesses subject to CCPA must provide consumers with four different types of notice:

1. Notice at collection
2. Notice of right to opt out (e.g., "Do Not Sell or Share My Personal Information" link)
3. Privacy Notice/Policy
4. Notice of financial incentive (as applicable)

Businesses should be mindful of the statutory requirements for each notice.

In addition to updating notices to include the proper disclosures as required by the CCPA, businesses must update contracts with third parties, service providers and contractors that may receive data from, or collect data on behalf of, businesses. Contracts must include specific language as mandated by the law.

The CPRA also added a definition of "share" to expressly address lingering confusion over "sales" of personal information under the CCPA – and to ward off further arguments that sharing personal information for cross contextual behavioral advertising in the adtech space is not a "sale" under the CCPA. Consumers have rights to opt-out of having their information shared or sold and some businesses are required to include a "Do Not Sell or Share My Personal Information" link on their sites.

The CPRA established a new broad category of "sensitive data". The definition is overly-inclusive, spanning from race, religion, and sexual orientation to financial account information and government identifiers (e.g. social security numbers). Consumers have specific rights in relation to their sensitive data, depending on the business' use of the data, as noted below.

Businesses must ensure that their privacy policies provide disclosures for consumers to exercise their privacy rights, including:

- **Right of access:** consumers have the right to request that a business disclose the categories of personal information collected; the categories of sources from which personal information is collected; the business or commercial purpose; the categories of third parties with which the business shares personal information; and the specific pieces of personal information the business holds about a consumer.
- **Right to opt-out** (or right to opt-in for minors) of sales or sharing of personal information.
- **Right to request deletion**: consumers have the right to request deletion of their personal information, but only where that information was collected from the consumer.
- **Right of non-discrimination** (i.e., to equal services and prices): the CCPA prohibits businesses from discriminating against consumers by denying goods or services, charging a different price or rate for goods or services, providing a different level or quality of goods or services, or suggesting that they will do any of these things based upon a consumer's exercise of any CCPA right.
- **Right to Correct**: Consumers have the right to correct inaccurate information. Businesses are required to use commercially reasonable efforts to correct inaccurate information.
- **Right to Limit Use and Disclosure of Sensitive Personal Information**: A consumer can request that a business use sensitive personal information only as necessary to perform the services or provide the goods or services, to provide certain services, and as authorized by further regulations.

- **Right to Portability**: A business is required to provide specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format. That information could then be transferred to another entity without hindrance.

Violation of the law is subject to civil penalties of not more than $2,500 for each violation or $7,500 for each intentional violation (e.g., per individual per violation, which can add up quickly). In certain limited circumstances of a data security breach, consumers have a private right of action.

Virginia: VCDPA

As mentioned above, VCDPA went into effect on January 1, 2023, but no enforcement date has been provided. Like other privacy laws, VCDPA adopted 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.

The VCDPA also addresses Sensitive Data. "Sensitive Data" means a category of personal data that includes: (1) personal data *revealing* racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (2) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; (3) the personal data collected from a known child (under the age of 13); or (4) precise geolocation data. VCDPA imposes limits on processing sensitive data such that doing so is prohibited absent consumer consent (opt-in).

Under the VCDPA, a sale of personal data means the exchange of personal data for monetary consideration by the controller to a third party. Unlike the CCPA, under which a sale occurs where personal data is exchanged for "monetary or other valuable consideration," the VCDPA requires that the consideration must be monetary to qualify as a sale of data.

Businesses must ensure that their privacy policies provide for individuals to exercise their rights[1], including:

- **Right of access**
- **Right to opt-out:** Consumers have the right to opt-out of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer (e.g. provision or denial of financial services).
- **Right to request deletion**
- **Right to data portability**
- **Right to correction**
- **Right of non-discrimination**

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.

Conclusion

If your business missed updating its policies and procedures prior to January 1, 2023, you should 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.

[1]Unless otherwise specified, each listed privacy right is essentially the same as CCPA.

For more information, please contact Chiara Portner.