INNOVATIVE DRIVEN

State Privacy Law

2023 Checklist for CRPA and Compliance

Over the past few years, companies have been dedicating significant resources to ensure compliance with the California Consumer Privacy Act (CCPA). With other states following suit, companies are now faced with becoming compliant with, California Privacy Rights Act (CPRA), Virginia Consumer Data Protection Act (VCDPA).

Luckily, you don't have to tackle this alone. We created a checklist to help you get started on your privacy compliance journey.

✓ Determine which state privacy law(s) apply to your business

CPRA, effective January 1, 2023, applies just like CCPA—applicable to all for-profit businesses that do business in California and meet the revenue or collection thresholds and for which an exception does not apply.

VCDPA (effective January 1, 2023) and CPA (effective July 1, 2023) apply to any for-profit business that conducts business in, or produces products or services targeted to residents of, Virginia or Colorado, and meets one of the following conditions, subject to exceptions:

a. Annually controls or processes the personal information of 100,000 or more state residents; or
b. Controls or processes personal data of at least 25,000 state residents and Virginia: derives over 50% of gross revenue from the sale of personal data. Colorado: derives revenue or receives a discount on the price of goods or services from the sale of personal data.

Employment and business-to-business exemptions. Both the VCDPA and the CPA exempt personal information collected from employees, applicants, officers, directors, contractors, and business representatives. The CPRA extends the CCPA's limited exemption on these categories, but only through January 1, 2023.

✓ Create a process for new right to correct consumers' personal information

All three states provide consumers with a new right to correction. To effectuate this right, businesses shall process a consumer's right to correct inaccuracies in the consumer's personal information.

✓ Build in processes for new opt-out rights— advertising and sharing

For all states, businesses must implement a means for consumers to opt out of the processing of their personal information for purposes of the following:

a. Sharing of their personal information used for "cross-context behav ioral advertising," even where no money is exchanged between the business and the third party—with requirement for a "Do Not Sell or Share My Personal Information" link added to a company's homepage (CPRA);
b. Targeted advertising (VCDPA and CPA)
c. Profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer (VCDPA and CPA)

✓Create a process to provide disclosed information to consumers

a. In response to a verifiable request, businesses are required to provide the 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 commonly used format. (CPRA, VCDPA, and CPA)
b. The CPRA provides for the right to know what information was collected on or after January 1, 2022, unless doing so proves impossible (i.e., a shorter data retention period) or would involve a disproportionate effort, which extends the current 12-month lookback period for requests to know under the CCPA. (CPRA)
c. Neither the VCDPA nor the CPA set an express time period for how far back a consumer's portability request may extend, so it can be presumed that portability obligations cover all person al information collected beginning on the date those statutes go into effect.

✓Develop a process for processing sensitive personal information

Virginia and Colorado require affirmative consent required to process a consumer's sensitive personal information. The CPRA does not impose an opt-in requirement to process sensitive personal information, but it does require businesses to honor a Californian's request to limit the use of their sensitive personal information.

a. Businesses must provide a clear and conspicuous link on their homep age—titled "Limit the Use of My Sensitive Personal Information"—that enables a consumer to limit the use or disclosure of their sensitive personal information.

By 2024, the CPA requires businesses to provide consumers with a universal opt-out option that allows a resident to click one button to exercise all opt-out rights. No such requirement exists under the CPRA or VCDPA.

✓Create an appeal process for consumer requests

Both the VCDPA and the CPA provide consumers with the right to appeal a business's denial to take action within a reasonable time period. There is no comparable right to appeal in California.

a. Under the VCDPA, within 60 days of receiving an appeal, a business must inform the consumer in writing of its response to the appeal and, if the business denies the appeal, it must provide the consumer with an "online mechanism," if available, or other method through which the consumer may contact the Virginia Attorney General to submit a complaint.
b. Under the CPA, businesses must provide an appeal process that is conspicuously available and easy to use. If an appeal is denied, the law requires the business to inform the consumer of their ability to contact the Colorado Attorney General if they have concerns about the result of the appeal.

✓Revise privacy policies

Businesses must disclose in their privacy policies— at or before the point of collection—the following:

a. The categories of sensitive personal information collected and whether that information is sold or shared. (CPRA)
b. The length of time the business intends to retain each category of personal information or, if that is not possible, the criteria used to determine that period. (CPRA)
c. Any business that processes person al information for targeted advertising must clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing (VCDPA and CPA)
d. How consumers can exercise their right to appeal a business's decision with regard to the consumer's request (VCDPA and CPA)

Revisions necessary to describe the new rights and processes identified above.

✓Assess relationships with service providers and data processors

Contracts between a business and a data processor shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. (CPRA, VCDPA, CPA)

a. In California, contracts with service providers must also prohibit the service provider from (1) selling or sharing the business's personal information; (2) retaining, using, or disclosing personal information outside of the direct business relationship between the service provider and the business; and (3) combining personal information received from one business with information received from another business.

b. In California, businesses will need to enter into a contract with any entity to which they disclose personal information, including third parties to which they sell personal information. The contract must include certain provisions, including (1) limiting use to specified purposes, and (2) providing the same level of privacy protections as required by the CPRA.

The CPRA obligates businesses fulfilling legitimate deletion requests to also notify contracted service providers or other third parties to delete the consumer's personal information from those third-party records.

✓Conduct risk assessments and implement data protection requirements

Businesses are required, under certain circumstances, to conduct risk assessments to weigh the benefits resulting from the processing of consumers' personal information.

a. The CPRA requires any business that processes consumers' personal information in a manner that presents "significant risk" to consumers' privacy or security to perform periodic (1) privacy risk assessments and (2) independent cybersecurity audits.

b. Virginia and Colorado require a mandatory data protection assessment for any of the following processing activities involving personal informa tion: (1) sale of personal information, (2) processing of sensitive personal information, and (3) targeted advertising.

✓Ensure data minimization and retention requirements are met

a. California, Colorado, and Virginia all establish data minimization principles and purpose limitations on a business's ability to collect personal information.

b. Businesses shall not retain a con sumer's personal information or sensi tive personal information for each disclosed purpose for a period longer than is reasonably necessary and proportionate to achieve its stated purposes.

Naheed Bleecker
414.975.0614
naheed.bleecker@innovativedriven.com