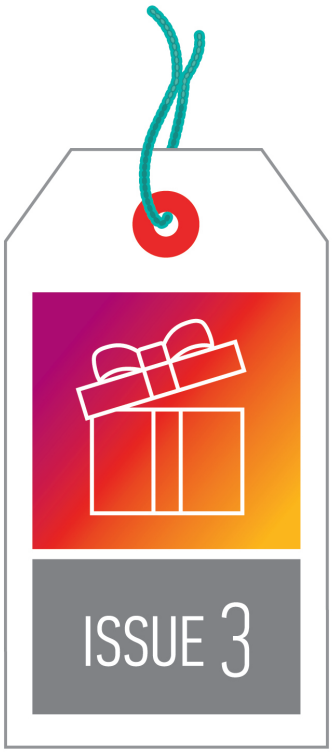
Updates



ft That Keeps on Giving?

Though it was not long ago that resolutions of California Consumer Privacy Act (CCPA) readiness ushered in the new year, 'tis the season once again to deck the halls with privacy compliance checklists. Retailers doing business in the United States have one year to prepare for the chorus of new comprehensive privacy laws that come into force in 2023: the California Consumer Privacy Rights Act (CPRA), which amends the existing CCPA, the Colorado Privacy Act (CPA), and the Virginia Consumer Data Privacy Act (VCDPA). What tidings do these three legislative updates bring? In this update, we describe the laws' key features and how they affect brands and retailers.

Timeline for Compliance

Retailers considering a single "universal" privacy program should set a deadline of January 1, 2023. Both the CPRA and VCDPA become operative on that date, with the CPA following on July 1, 2023. And notably, though most of the CPRA's substantive provisions won't become effective until January 1, 2023, personal information collected by businesses starting on January 1, 2022, will be subject to the CPRA's requirements (with some exceptions).

Deadlines for state regulations and guidance vary. The Virginia Consumer Data Protection Work Group, tasked with identifying areas of potential amendment to the VCDPA, submitted a report on November 1, 2021, that the Virginia legislature will consider in its 2022 session. The CPRA requires that final regulations be adopted by July 1, 2022; however, the California Privacy Protection Agency (CPPA), which has commenced preliminary rulemaking activities, has suggested that meeting the deadline may be challenging. Meanwhile, the CPA gives the Colorado attorney general until January 1, 2025, to adopt guidelines for CPA compliance.

What's New?

The good news is that work done to comply with the CCPA can be leveraged for the CPRA, VCDPA, and CPA. Nonetheless, each law presents new rights and obligations that will require retailers to revisit their compliance programs. The list below highlights new obligations that go above and beyond the CCPA.

- **Employee and B2B Data.** The employee and business contact exemptions provided by the CCPA sunset with the CPRA. As a result, many obligations currently owed only to California consumers under the CCPA will be extended to all California residents, with some exceptions. The VCDPA and CPA, however, generally do not apply to employee and business contact data.
- **Sensitive Personal Information.** Each law imposes opt-in (VCDPA and CPA) or opt-out (CPRA) requirements related to the use of "sensitive personal information." While the definition of sensitive personal information varies across the three states, common denominators include biometric information, data that reveal race or ethnicity, mental or physical health condition, or sexual orientation.
- **Consumer Rights.** In addition to the opt-in/opt-out rights mentioned above, residents of these three states have several new rights, including, among others, the right to (1) correct inaccurate personal information, (2) opt out of the use of their personal information for certain profiling activities, and, in Virginia and Colorado, (3) appeal the denial of their consumer rights request.
- **Selling, Sharing, and Targeted Advertising.** Retailers familiar with "Do Not Sell" requirements under the CCPA will be well positioned to comply with the similar restrictions found in each of the new state laws. The laws go further, however, in also requiring opt-outs for targeted advertising (called "sharing" by the CPRA). Take note, too, of requirements to honor user-enabled universal opt-out mechanisms, like the Global Privacy Control (GPC). The CCPA regulations already require businesses to treat user-enabled global privacy controls as a valid request to opt out of sales, and the California Attorney General's Office has taken the position that honoring GPC satisfies this requirement. Further, honoring universal opt-outs will be required under both the CPRA and CPA. Stay tuned for further rulemaking in California and Colorado on this topic.
- **Data Protection Assessments.** Each of the new state laws contemplates documented privacy risk assessments for processing activities that present a heightened risk of harm to consumers. Under the VCDPA and CPA, for example, data protection assessments will be required for targeted advertising, processing of sensitive personal information, and more.
- **Data Minimization/Purpose Limitation.** Under the CPRA, VCDPA, and CPA, organizations must limit their processing of personal information to that which is "reasonably necessary" and "proportionate" to achieve the intended purpose. Retailers will need to establish data retention policies and schedules to meet these requirements and ensure that personal information is not retained longer than permitted by applicable law.
- **Contractual Requirements.** As with the CCPA, the new state privacy laws specify contractual obligations that must be imposed on third parties (service providers, processors, contractors, etc.) receiving personal information.

What Should Retailers Do Now?

- **Determine if the CPRA, VCDPA, and CPA Apply.**[1] Retailers already subject to the CCPA will likely still be subject to the CPRA, though the processing thresholds have changed slightly. As with the CCPA, retailers without a brick-and-mortar presence in Virginia and Colorado may still be subject to the VCDPA and CPA. The VCDPA and CPA apply to organizations that operate in Virginia or Colorado, respectively, or that target goods and services to residents of those states, subject to satisfying specified processing

thresholds.

- **Assess Current Privacy Practices.** Understanding an organization's information practices is key, even for retailers that have already developed CCPA compliance programs. Data mapping (or updating an existing data map) is essential to identifying new types and uses of personal information covered by each law, particularly employee and business contact data and sensitive personal information. Critically, data mapping can also help identify categories and uses of personal information that may be totally or partially exempt, for example, personal information regulated by Health Insurance Portability and Accountability Act (HIPAA). Retailers should also assess their use of personal information to determine what opt-out rights may need to be provided, particularly for sales and targeted advertising. Perkins Coie offers a proprietary data mapping solution, Data Navigator, that can help an organization complete this exercise.
- **Update External Privacy Disclosures.** Plan to update and roll out consumer-facing privacy notices. In addition to updating the organization's customer-facing privacy policy, there may be a need to provide employee and job applicant privacy policies, just-in-time privacy notices, and opt-out notices for sales and targeted advertising.
- **Consumer Rights.** Revisit the organization's "Do Not Sell" mechanism and ensure it is providing an opt-out option for any targeted advertising that may be occurring. Additionally, review and update user interfaces and related processes for consumer rights requests to ensure compliance with new opt-in, opt-out, correction, appeal, and other rights.
- **Commercial Contracts.** Take an inventory of the organization's vendor contracts and prepare to update contracts with service providers, contractors, and other third parties that buy or receive personal information to ensure appropriate restrictions and obligations are in place.
- **Internal Governance.** Establish and document internal governance policies and procedures to comply with obligations under the new laws, including data minimization and purpose limitation requirements. Ensure that all personnel receive data protection training, with specialized training for personnel tasked with handling sensitive information or consumer rights requests.

Looking Ahead

Many other states are considering comprehensive privacy bills that could materialize in 2022. Perkins Coie has elves on the ground to keep a pulse on the evolving landscape. Please reach out to any of our Privacy attorneys for assistance.

Endnotes

[1] The applicability thresholds for each law are as follows:

The CPRA applies to any business that (1) exceeds $25 million in annual gross revenue in the preceding calendar year, (2) annually buys or sells or shares the personal information of 100,000 or more consumers or households, or (3) derives 50% or more of its annual revenue from selling or sharing consumers' personal information. Like the CCPA, the CPRA will also apply to any entity that controls or is controlled by a business that meets the foregoing requirements, shares common branding with the business, and with whom the business shares consumers' personal information.

The VCDPA applies to any for-profit entity that does business in Virginia or that targets products and services to residents of Virginia and that (1) during a calendar year, controls or processes personal data of at least 100,000 consumers, or (2) controls or processes personal data of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal data.

The CPA applies to any entity that does business in Colorado or that targets products and services to residents of Colorado and that satisfies one or both of the following thresholds: (1) controls or processes the personal data of 100,000 or more consumers during a calendar year; or (2) 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 or more consumers.

Authors

Explore more in

Privacy & Security Retail & Consumer Products

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law