Kramer Levin

ALERT APRIL 8, 2021

How To Confirm Your Privacy Program Complies With California and Virginia Privacy Obligations

Introduction

Consistent with a growing national trend, Virginia joined California in recently passing consumer privacy legislation with broad national reach. Both the Virginia Consumer Data Protection Act (Virginia CDPA) and the California Privacy Rights Act (CPRA) take effect on Jan. 1, 2023, following closely behind the recently passed and enacted California Consumer Privacy Act (CCPA), which went into effect in January 2020. Kramer Levin developed the following checklist to help businesses better understand:

- Whether these laws apply to your business
- What consumer rights they create
- How to respond to consumers exercising these rights
- The best practices to streamline and ensure business compliance

For companies that have already implemented the CCPA, the good news is that there is significant overlap in the Virginia CDPA compliance obligations — as well as overlap with the CPRA's additional obligations on companies within its scope. Thus, if a business is already in compliance with California's privacy laws, it will also satisfy many requirements of the Virginia CDPA. However, as discussed below, the Virginia CDPA does differ in some respects.

We will continue to monitor the latest developments and update our checklists accordingly. Please reach out to the Kramer Levin privacy team for additional assistance.

Checklist for the California Consumer Privacy Act (CCPA)

1. Does the CCPA Presently Apply to Your Business?

- The CCPA currently applies to entities that do business in California and meet at least one of the following conditions:
    - Have $25 million in annual gross revenue

- Annually handle the personal information of 50,000 or more consumers, households or devices
- Derive 50% or more of their annual revenues from selling personal information

2. If Yes, the Company Must Provide Notices to Consumers of the Following Rights:

- The Right to Notice Before Collection of Personal Information
- The Right to Know What Has Been Collected
- The Right to Know What Is Sold or Disclosed, and to Whom
- The Right to Opt-Out of Sale
- The Right to Deletion
- The Right to Non-Discrimination

3. If Yes, the Company Must Also:

- Update its Privacy Policies to include specific information, including notice of the consumer rights listed above
- Provide at least two methods for consumers to submit CCPA requests or exercise these rights
- If the company sells personal information, provide a web link for consumers to opt-out of the sale of their personal information that is easy for consumers to execute and shall require minimal steps

4. Responding to Consumer Requests

- Businesses should implement procedures for responding to consumer requests, including:
  - How to verify the authenticity of the request
  - Determine what categories of information to disclose after a verified request, including whether different levels of verification will be required for different levels of sensitive information
  - Maintain records of all consumer requests and responses for 24 months

5. Recommended Best Practices for CCPA Compliance

- First, map what data your business:
  - Collects
  - Processes and stores

    - Shares with third parties, including vendors

- Review and update:
    - Data retention policy
    - Security policy
    - External privacy policy
- Note that the CCPA provides a private right of action for data breaches that result from failing to maintain reasonable security procedures and practices
- Review and update agreements with third parties that receive consumers' personal information from the business. Include provisions that:
    - Classify vendors, contractors and other third parties as "service providers"
    - Make clear that they must also comply with the CCPA

Checklist for the California Privacy Rights Act (CPRA)

All right. So now the company has considered CCPA compliance and is feeling good about its privacy, data security and vendor management obligations, policies and procedures. But companies cannot stop there. The CPRA comes online Jan. 1, 2023, and will both modify the CCPA and establish new obligations for companies within its scope.

1. Does the CPRA Apply to Your Business?

- The CPRA takes effect Jan. 1, 2023, and will apply to entities that do business in California and meet at least one of the following conditions:
    - Have $25 million in annual gross revenue
    - Annually handle the personal information of 100,000 or more consumers
    - Derive 50% or more of their annual revenues from selling *or sharing* personal information
- Note this changes the scope and reach of the California consumer privacy legislation — requiring a larger business footprint on data collection than its predecessor CCPA did before triggering obligations under the second prong.

2. New Consumer Rights

- The CPRA will add the following new rights to the existing consumer rights under the CCPA:
    - Error correction:

        - Providing data subjects with the right to ask a business to correct inaccurate personal information.
    - Data portability:
        - Providing data subjects with the right to request transmission, in a machine-readable format, of the specific pieces of personal information a business has collected about a consumer.
    - Sensitive Personal Information:
        - Providing data subjects with the right to limit the use of a new subcategory of information, called "Sensitive Personal Information." This category includes government identifiers, account and login information, precise geolocation data, racial or ethnic origin, religious or philosophical beliefs, union membership, contents of mail, email, and text messages, genetic data, sexual orientation, and health or biometric information. This concept will be familiar to companies that are within the ambit of the GDPR.
    - Opt-out of sale *or sharing*:
        - Presently, the CCPA requires businesses that sell personal information to provide an opt-out link; with the implementation of the CPRA, companies will have to provide the same right when they share such information.

3. Update Your Notices and Privacy Policies

- The CPRA requires businesses to make additional changes and disclosures to their notices and policies:
    - If the company shares information, it must update its opt-out links accordingly
    - If the company sells or shares personal information, or uses sensitive personal information for purposes other than those necessary to provide the requested goods or services, it must provide a link on the business's homepage titled "Limit the Use of My Sensitive Personal Information"
- Businesses must also include the following new information in their privacy policies:
    - Whether the business collects Sensitive Personal Information and, if so, what categories.
    - If the business uses Sensitive Personal Information for purposes not necessary to provide the requested goods or services, it must notify the consumer of those extraneous uses and of the consumer's right to limit such use.

- The length of time a business intends to retain each category of information, including Sensitive Personal Information if applicable.
- Notice to consumers of their right to correct inaccurate information.

4. Complying With the CPRA

- In order to comply with the CPRA, businesses should make the following adjustments to their existing procedures for responding to CCPA requests:
  - Establish procedures for informing all service providers, contractors or third parties of a consumer's request to delete any information that the business has shared with the third party
  - Establish procedures for correcting inaccurate personal information at a consumer's request
  - Use "commercially reasonable efforts" to correct any inaccurate personal information identified by the consumer
  - Establish procedures for transmitting specific pieces of personal information to a consumer on request
  - Keep accurate records of the categories and specific pieces of personal information the business has collected about consumers, in order to respond to a consumer request for such information, which may exceed the immediately preceding 12 months under the CPRA
  - Implement or update service provider agreements
    - Note that the CPRA requires a business that shares personal information with third parties to enter into written agreements that cover specific duties on both sides, including the limited purposes for such sharing and the third party's obligation to comply with the CPRA.
  - Implement reasonable security procedures and practices appropriate to the nature of the personal information, to protect it from unauthorized or illegal access or destruction

Checklist for Virginia's Consumer Data Protection Act (Virginia CDPA)

If the company has assessed and applied all of the above, management may feel on top of consumer privacy. But wait! Virginia has now passed its own incredibly robust privacy law. It too will onboard on Jan. 1, 2023, and will require additional steps to achieve full compliance on top of a CPRA-compliant program.

1. Does the Virginia CDPA Apply to Your Business?

- The Virginia CDPA applies to all entities that "conduct business" in Virginia or "produce products or services that are targeted to residents" of Virginia and meet either of the following conditions:
    - Control or process personal data of at least 100,000 consumers (defined as residents of Virginia)
    - Control or process the data of at least 25,000 consumers and derive over 50% or more of their gross revenue from selling personal data
- Unlike California's CCPA and CPRA, Virginia does not include a blanket revenue threshold. Thus, even large businesses will not be subject to the Virginia CDPA unless the business processes the data of a minimum number of Virginia residents.

2. Exemptions

- The Virginia CDPA exempts the following five types of entities:
    - Virginia state bodies and agencies
    - Financial institutions or data subject to the Gramm-Leach-Bliley Act (GLBA)
    - Covered entities or business associates under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act
    - Nonprofit organizations
    - Institutions of higher education

3. Consumer Rights

- Similar to California's CCPA and CPRA, the Virginia CDPA grants consumers the following rights:
    - The Right to Access (i.e., obtain a copy of personal data previously provided to the controller)
    - The Right to Correct Inaccuracies
    - The Right to Deletion
    - The Right to Portability (i.e., receive a copy of personal data in a readily usable format that can be transferred to another controller)
    - The Right to Know What Has Been Collected
    - The Right to Opt-Out of Sale

        - Virginia's CDPA limits the definition of "sale" to the exchange of personal data for "monetary" consideration, unlike the CCPA, which broadly defines sale as any involving "valuable" consideration. And note the CPRA will expand opt-out to simply sharing such information in January 2023.
    - The Right to Non-Discrimination
- In comparison to California's CCPA and CPRA, the Virginia CDPA grants Virginians the following additional consumer rights:
    - The Right to confirm whether a controller (typically the original collector of the data and the company that directs its use) is processing personal information
    - The Right to Opt-Out of any processing of their personal data for targeted advertising
    - The Right to Opt-Out of any processing of personal data for the purposes of profiling for decisions that produce legal significant effects concerning the consumer
    - The Right to Opt-In to processing of "sensitive data"
    - The Right to Appeal a Business's Refusal of Consumer Privacy Requests

4. Recommended Best Practices for Virginia CDPA Compliance

- Businesses must develop procedures to **respond to consumer requests** to exercise their rights, including:
    - Ability to respond to requests within 45 days.
        - If a business needs an extension, it must still respond to the consumer during the first 45-day period and provide a reason for the delay.
    - Allow consumers two free inquiries annually.
    - Procedure for declining a request if the business cannot authenticate the consumer's identity or if the data requested is not subject to the statute (e.g., employment data).
    - Establish a "conspicuously available" appeals process for consumers who exercise rights granted by the Virginia CDPA but are denied by the business.
        - The right to appeal is not included in California's CCPA or CPRA.
    - Within 60 days of receiving an appeal, the business must inform the consumer in writing of its response to the appeal, including a written explanation of the reasons for the decision.
    - If the controller denies the appeal, the business must also provide the consumer with an "online mechanism or other method" through which the consumer can submit a complaint to the attorney general.

5. Technical Safeguard Requirements

- Businesses must develop the following **technical procedures** to comply with the Virginia CDPA:
    - Post a privacy notice that discloses, at a minimum:
        - The categories of personal data collected
        - The purposes for processing personal data
        - How consumers can exercise their rights with respect to their personal data (including how to appeal any decision by the business with respect thereto)
        - Categories of personal data shared with third parties, if any
        - Categories of third parties, if any, with whom the business shares personal data
        - Whether personal data is sold to third parties and how to opt-out
        - Whether personal data is used for targeted advertising and how to opt-out
    - Limit data collection to what is adequate, relevant and reasonably necessary for the disclosed purposes
    - Obtain a consumer's consent before processing any sensitive data
    - Establish and implement reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data
    - Conduct a formal "data protection assessment" of all data collection and processing activities involving personal data that is:
        - Used for purposes of targeted advertising
        - Sold
        - Used for purposes of profiling
        - Sensitive data
        - Any activity involving personal data that presents a "heightened risk of harm to consumers"
    - Controllers must enter into Data Processing Agreements (DPAs) with their data processors.
        - These agreements must "clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of the processing, and the rights and obligations of both parties."
        - The Virginia CDPA provides specific terms that must be included in any DPA.

Key Differences Between the Virginia and California Privacy Statutes

If the company is CCPA- and CPRA-compliant, some key takeaways for implementing the Virginia CDPA are:

- **The Virginia CDPA does not apply to company employee data or data transferred to third-party processors in a business-to-business context:** Under the Virginia CDPA, a "consumer" includes only Virginia residents acting in an "individual or household context" and notably excludes "any person acting in a commercial or employment context." Therefore, unlike the California laws, the consumer rights do not extend to company employee data or business-to-business (B2B) data.

- **The Virginia CDPA expands individual rights:** The Virginia CDPA includes rights beyond those provided in California, including the right to opt-out of processing personal data for purposes of targeted advertising.

- **The Virginia CDPA defaults to prohibiting the processing of sensitive information:** Under the Virginia CDPA, consumers must first opt in to allow processing of their sensitive information. By contrast, California consumers must affirmatively opt-out to prevent such processing.

- **No private right of action under the Virginia CDPA:** The Virginia CDPA does not grant a private right of action for data security incidents, unlike the California laws. Instead, the Virginia CDPA grants the attorney general exclusive authority of enforcement, who may seek injunctive relief and damages for up to $7,500 for each violation as well as "reasonable expenses incurred in investigating and preparing the case, including attorney fees." This means that even where there has been a breach or security incident, consumers cannot bring claims pursuant to the Virginia CDPA.

- **Safe harbor:** The Virginia CDPA allows a business 30 days to correct deficiencies after notice from the attorney general. While the CCPA provided the same notice and cure period, California's CPRA does away with that safe harbor period.

Authors and Editors

Samantha V. Ettari
Special Counsel
T 212.715.9395
settari@kramerlevin.com

Alan R. Friedman
Partner
T 212.715.9300
afriedman@kramerlevin.com

Kevin M. Moss
Counsel
T 212.715.9224
kmoss@kramerlevin.com

Austin Manes
Associate
T 650.752.1718
manes@kramerlevin.com

K. Kaelin Brittin
Law Clerk
T 212.715.9545
kbrittin@kramerlevin.com

Martin M. McSherry
Law Clerk
T 212.715.9122
mmcsherry@kramerlevin.com