FEBRUARY 13, 2023 | AI/TECHNOLOGY, PRIVACY & DATA SECURITY

New State Privacy Laws in California and Virginia Are Now Effective

By Darius Rohani-Shukla

There have been important developments in data privacy laws as both the Virginia Consumer Data Protection Act ("VCDPA") and California Privacy Rights Act ("CPRA") are now in effect. Both laws are remarkably expansive and require careful attention to achieve compliance.

The Virginia Consumer Data Protection Act (VCDPA)

The Virginia Consumer Data Protection Act (VCDPA) applies to any person or business that conducts business in Virginia and processes personal data of Virginia residents.

Who does the VCDPA apply to?

Under the VCDPA, obligations are imposed on entities that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that either:

- Control or process the personal data of at least 100,000 consumers during a calendar year.
- Control or process the personal data of at least 25,000 consumers and derive at least 50% of its gross revenue from the sale of personal data.

Personal data is linked or reasonably linkable to an identified or identifiable natural person. This includes, but is not limited to, names, addresses, email addresses, IP addresses, and other unique identifiers.

What does the VCDPA require employers to do?

The VCDPA requires employers that conduct business in Virginia and process personal data of Virginia consumers (natural persons are residents of the Commonwealth acting only in an individual or household context) to take specific measures:

- **Limit Data Collection:** Controllers must limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer.
- **Establish a Consumer Request Process:**Controllers must establish one or more secure means for consumers

to submit requests to exercise their rights (listed below) and describe them within a privacy notice.

- **Provide Privacy Notices:** Companies must provide privacy notices to Virginia residents regarding their personal information, including what categories of personal information are being collected, the purposes for which the information will be used, information related to personal data shared with third parties, and Virginia consumer rights concerning the use of their personal information.
- **Implement Security Measures:** Controllers must establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.
- **Obtain Consent for Processing Sensitive Data:**Controllers are required to obtain the consumer's consent before processing any sensitive data.
- **Conduct Data Protection Assessments:** Controllers must conduct and document a data protection assessment for certain processing activities, including the sale of personal data, the processing of personal data for purposes of targeted advertising or profiling, the processing of sensitive data and any processing activities involving personal data that present a heightened risk of harm to consumers. Data protection assessments must identify and weigh the benefits to the business of processing consumers' data against potential risks to consumers associated with such processing.
- **Enter into Data Processing Agreements (DPAs).** Controllers must enter into 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 processing, and the rights and obligations of both parties." The VDPA provides specific terms that must be included in any DPA.

What rights does the VCDPA provide consumers?

Consumers have the following rights under the VCDPA:

- **Right to access:** Consumers have the right to confirm whether a controller is processing the consumer's personal data and obtain access to such data.
- **Right to correct:** Consumers have the right to correct inaccuracies in the consumer's personal data.
- **Right to delete:** Consumers have the right to delete personal data provided by or obtained about the consumer.
- **Right to data portability:** Consumers have the right to obtain a copy of the consumer's personal data in a portable and readily usable format.
- **Right to opt out of certain data processing:** Consumers have the right to opt out of the processing of personal data for purposes of: (i) targeted advertising; (ii) the sale of personal data; or (iii) profiling in further of decisions that produce legal or similarly significant effects concerning the consumer.

Note: The following entities are exempt the VCDPA (1) financial institutions subject to Gramm-Leach-Bliley Act, (2) entities regulated by HIPAA, (3) non-profits, (4) Virginia state agencies, and (5) colleges and universities.

The California Privacy Rights Act (CPRA)

The CPRA was a ballot initiative that California voters passed in November 2020, and amended and expanded

California's previous privacy law, the CCPA. It took effect on January 1, 2023. Previously, the CCPA exempted employee data from its consideration. Under the CPRA, that exemption was not extended and employers are required to provide disclosures and notices to employees regarding their personnel information.

Who does the CPRA apply to?

The CPRA applies to for-profit companies that do business in California and meet one or more of the following criteria:

- Have annual gross revenues in excess of $25 million;
- Buy, receive, sell, or share the personal information of 100,000 or more consumers, households, or devices for commercial purposes; or
- Earn more than half of their annual revenues from selling consumers' personal information.

What does the CPRA require employers to do?

The CPRA requires specific measures to be taken by companies that conduct business in California:

- **Provide Privacy Notices:** Employers must prepare and provide a privacy notice to any employee and/or job applicant at or before the time personal information is collected. The notice must include:

  (a) the categories of sensitive personal information collected;

  (b) whether that sensitive personal information is sold or shared; and

  (c) the length of time the employer intends to retain each category of sensitive personal information.

- **Honor Consumer Requests:** Employers must honor consumer (employee) requests, such as the right to delete, know, correct, access, data portability, non-discrimination, limit the use and disclosure of sensitive personal information and the right to opt-out of both the sale and sharing of personal information. Businesses must establish processes in order for employees to exercise their rights, and train employees to respond to potential requests or deny requests where appropriate. Businesses must understand how personal information is collected, used, and stored in order to respond to employee requests.
- **Safeguard Personal Information:** Employers must safeguard personal information against unauthorized disclosures and provide employees with the right to limit the use and disclosure of sensitive information.
- **Cybersecurity Audit:** Qualified employers must perform an annual cybersecurity audit if they perform processing activities that are likely to result in a significant risk to an individual's privacy.
- **Data Breach Notification**: *Businesses must notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. The disclosure* "shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement."
- **Enter Data Processing Agreements:** Employers must enter into a Data Processing Agreement ("DPA") when it (1) discloses personal information to a service provider, (2) discloses personal information to a contractor, or (3) sells or shares personal information to a third party. This requirement applies regardless of the types of

personal information processed (i.e., employment related or otherwise).

What rights does the CPRA provide consumers?

Consumers have the following rights under the CPRA:

- Right to know (request disclosure of) personal information collected by the business about the consumer, from whom it was collected, why it was collected, and, if sold, to whom;
- Right to delete personal information collected from the consumer;
- Right to opt-out of the sale of personal information (if applicable);
- Right to initiate a private cause of action for data breaches;
- Right to correct inaccurate personal information; and
- Right to limit use and disclosure of sensitive personal information.

What do the terms *Personal Information* and *Sensitive Personal Information* mean?

Personal Information is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Sensitive Personal Information is a subset of personal information newly defined in the CPRA. SPI is personal information that reveals: a consumer's social security, driver's license, state identification card, or passport number, a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account, a consumer's precise geolocation, a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership, the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication, or a consumer's genetic data.

Exemptions: The CPRA does not apply where: the business must comply with legal obligations, most often related to criminal investigations; deidentified or aggregate data is processed; the sale, sharing, or collection of data happened outside of California; personal information is collected in clinical trials; personal information is collected in an emergency; or personal information processed is under the scope of the California Confidentiality of Medical Information Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, California Financial Information Privacy Act, the Federal Farm Credit Act, or the Driver's Privacy Protection Act.

Who enforces the CPRA? What are the fines for non-compliance?

The California Privacy Protection Agency (CPPA) enforces the CPRA. CPRA fines are up to $2,500 for violations per consumer and up to $7,500 for intentional breaches per consumer.

Conclusion

As a business, it is important to ensure compliance with the VCDPA regarding the personal data of Virginia residents, and CPRA regarding employee and other personal data of California residents.

Please let us know if you have any questions or concerns regarding the VCDPA or CPRA and how it may affect

your business.