Computer & Communications Industry Association
Tech Advocacy Since 1972

Virginia's "Consumer Data Protection Act" Summary

On March 2, 2021, Governor Northam signed SB1392, the "Consumer Data Protection Act" ('VCDPA') into law. The Act's provisions take effect on January 1, 2023. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	• The VCDPA applies to controllers that conduct business in the Commonwealth or produce products or services that are **targeted** to residents of the Commonwealth and that (1) during the preceding calendar year, control or process personal data of at least 100,000 consumers **or** (2) control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.
Covered Data	• **"Personal data"** means information that is linked or reasonably linkable to an identified or identifiable natural person and does not include de-identified data or publicly available information. • **"Sensitive data"** means (a) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (b) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; (c) personal data collected from a known child; or (d) precise geolocation data.
Key Definitions	• ***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. • ***"De-Identified Data"***: data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such a person. • ***"Pseudonymous Data"***: personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. • ***"Targeted Advertising"***: displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. • ***"Sale of Personal Data"***: the exchange of personal data for monetary consideration by the controller to a third party. A sale of personal data does not include: (1) disclosure to a processor that processes the personal data on behalf of the controller; (2). disclosure to a third party to provide a product or service requested by the consumer; (3) disclosure to an affiliate of the controller;(4) disclosure of information that the consumer intentionally made available and did not restrict; or (5) disclosure to a third party as an asset that is part of a merger, acquisition, or bankruptcy.
Consumer Rights	• **Affirmative Consent**: A controller shall not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA. • **Access**: A consumer has the right to confirm whether or not a controller is processing the consumer's personal data and to access such personal data. • **Correction**: A consumer has the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data. • **Deletion**: A consumer has the right to delete personal data provided by or obtained about the consumer. • **Portability**: A consumer has the right to obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance. • **Opt Out Rights**: A consumer has the right to opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
Business Obligations	• **Responding to Consumer Requests**: A controller shall comply with a request by a consumer to exercise the consumer rights authorized and shall respond to the consumer without undue delay, but in all cases within 45 days of receipt of the request submitted (may be extended once by 45 additional days when reasonably necessary). Information provided shall be free of charge up to twice annually per consumer (unless requests are manifestly unfounded, excessive, or repetitive). A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request. Within 60 days of receipt of an appeal, a controller shall

	inform the consumer in writing of any action taken in response to the appeal and provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint. • **Data Minimization**: A controller shall 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. • **Avoid Secondary Use**: A controller shall not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed unless the controller obtains the consumer's consent. • **Data Security**: A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue. • **No Unlawful Discrimination**: A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising consumer rights. • **Transparency**: A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes (1) the categories of personal data processed by the controller; (2) the purposes for processing personal data; (3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (4) the categories of personal data that the controller shares with third parties; (5) the categories of third parties, if any, with whom the controller shares personal data. • **Disclosure**: A controller shall clearly and conspicuously disclose the sale of personal data to third parties or processing of personal data for targeted advertising.
Data Protection Assessments	• A controller shall conduct and document a data protection assessment of (1) the processing of personal data for purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for purposes of profiling; (4) the processing of sensitive data; (5) any processing activities involving personal data that present a heightened risk of harm to consumers. The Attorney General may request that a controller disclose any data protection assessment relevant to an investigation.
Controller / Processor Distinction	• **A processor shall adhere to the instructions of a controller** and shall assist the controller in meeting its obligations under the VCDPA. A contract between a controller and a processor shall govern the processor's data processing procedures and shall 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 contract shall also include requirements that the processor shall (1) ensure that each person processing personal data is subject to a duty of confidentiality; (2) delete or return all personal data to the controller as requested at the end of the provision of services; (3) make available to the controller all information in its possession necessary to demonstrate the processor's compliance with obligations; (4) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; (5) engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor.
Exceptions	• A controller **may disclose pseudonymous data or de-identified data** with an exercise of reasonable oversight to monitor compliance with any contractual commitments. • The VCDPA shall not be construed to restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government authorities; (c) cooperate with law-enforcement agencies; (d) prepare for and defend legal claims; (e) providing a product or service requested by a consumer; (f) protect interests essential for life or physical safety of the consumer; (g) detect and protect against security incidents; (h) engage in scientific or statistical research in the public interest; (i) assist third parties with the obligations of the VCDPA. • Data exempt from the VCDPA includes protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, and COPPA.

Enforcement	• The **VCDPA does not provide the basis for, or be subject to, a private right of action** to violations of this Act. • The Attorney General shall have exclusive authority to enforce violations of the Act and shall provide a controller or processor 30 days' written notice identifying specific provisions being violated. Any controller or processor that violates the VCDPA is subject to an injunction and liable for a civil penalty of not more than $7,500 for each violation. All civil penalties collected under the VCDPA shall be paid into the state treasury and credited to the **Consumer Privacy Fund**, which shall be used to support the work of the Attorney General to enforce VCDPA.