

THE VIRGINIA CONSUMER DATA PROTECTION ACT (VCDPA)



The VCDPA (“the Act”) grants Virginia consumers individual rights and imposes corresponding obligations on covered businesses:

GDPR-LIKE CONTROLLER / PROCESSOR DISTINCTION

Like the EU GDPR, the Act distinguishes between:



Controllers: Entities that determine the purpose and means of processing personal data; and



Processors: Entities that process personal data on behalf of a controller. The Act imposes specific obligations and limitations on processors, and sets forth required contents of a written controller-processor contract.

INDIVIDUAL RIGHTS

- 1 Right to Know / Access.** Consumers may request that a controller confirm whether it processes personal data relating to the individual and provide access to that personal data.
- 2 Right to Correction.** Consumers may request that a controller correct inaccuracies in the consumer’s personal data.
- 3 Right to Deletion.** Consumers may request that a controller delete personal data *provided by or obtained about* the consumer.
➤ *Note:* This is not limited to personal data collected *from* the consumer, and the Act does not contain specific deletion exceptions.
- 4 Right to Data Portability.** Consumers may request to obtain a copy of the personal data *that they previously provided to a controller* in a portable and, to the extent technically feasible, readily usable format, where the processing is carried out by automated means.
- 5 Right to Opt Out.** Consumers may request to opt out of a controller’s processing of their personal data for targeted advertising, sale, or automated profiling in furtherance of decisions that produce significant effects.
- 6 Right to Appeal.** Consumers may appeal a controller’s denial of their individual rights requests. See “Controllers’ Obligations” for more.

CONTROLLERS’ OBLIGATIONS



Data Minimization. Controllers must limit their collection of personal data to what is adequate, relevant, and reasonably necessary for the purposes for which the data are processed, as disclosed to the consumer.



Purpose Limitation. Controllers are generally prohibited from processing personal data for purposes that are not reasonably necessary to, or compatible with, the disclosed purposes without the consumer’s consent.



Notice. Controllers must provide consumers with meaningful notice regarding the personal data they process, the personal data they share with third parties, if applicable, and how consumers may exercise their rights under the Act, including the right to appeal.



Consent. Controllers must obtain consent to process a consumer’s sensitive personal data (see flip side) and may only process the personal data of children *under age 13* in accordance with COPPA.



Data Security. Controllers must establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect personal data.



Non-Discrimination. Controllers may not process personal data in violation of state or federal discrimination laws, nor discriminate against consumers for exercising their rights under the Act.



Data Protection Assessments. Controllers must conduct and document data protection assessments for certain high-risk processing activities and make such assessments available to the Attorney General upon request.



Appeals Process. Controllers must establish a process for consumers to appeal denials of individual rights requests and make the process conspicuously available to consumers. A controller that denies an appeal must provide the individual with a mechanism to contact the Virginia AG.



THE VIRGINIA CONSUMER DATA PROTECTION ACT (VCDPA)







MORRISON
FOERSTER

WHO MUST COMPLY?




The Act applies to entities that conduct business in Virginia or produce products or services that are targeted to Virginia residents *and* that:

-  Control or process personal data of at least **100,000 consumers who are VA residents** in a calendar year; *or*
-  Control or process the personal data of at least **25,000 consumers who are VA residents** and derive over **50% of gross revenue** from the sale of personal data.

KEY DEFINITIONS

-  **Consumer:** a Virginia resident, but only to the extent that the individual is acting in an individual or household context.
 - Excludes individuals acting in a B2B or employment context.
-  **Personal Data:** information linked or reasonably linkable to an identified or identifiable *individual* (not a household or device).
 - Excludes de-identified and publicly available data, but note that a controller in possession of de-identified data must publicly commit that it will not attempt re-identification, among other conditions.
-  **Sensitive Data:** (i) personal data revealing racial or ethnic origin, religious beliefs, mental or physical diagnoses, sexual orientation, or citizenship or immigration status; (ii) genetic or biometric data for identification purposes; (iii) personal data collected from a child under 13 years of age; and (iv) precise geolocation data.
-  **Sale:** the exchange of personal data from a controller to a third party *for monetary consideration*.
 - Excludes sharing data with affiliates and certain other sharing.

EXCEPTIONS

-  **Entities:** The Act exempts non-profit organizations, institutions of higher education, utilities, financial institutions subject to Title V of the GLBA, and HIPAA-covered entities and business associates.
-  **Types of Personal Data:** The Act exempts personal data created or maintained in the employment context or for purposes of select federal laws, including HIPAA, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, and the Driver's Privacy Protection Act.
-  **Permitted Processing:** The Act does not restrict a controller or processor's ability to comply with laws or regulations or provide a product or service specifically requested by a consumer, among other purposes.

ENFORCEMENT

- ✓ **Virginia AG** has enforcement authority.
- ✓ **No private right of action**, even following data security incidents.
- ✓ Businesses have **30-day period** to cure alleged violations, upon receipt of AG notice.
- ✓ Thereafter, AG may seek civil penalties of up to **\$7,500 per violation**, injunctive relief, expenses, and attorney's fees.

MOFO CONTACTS



[Christine E. Lyon](#)
Partner, Palo Alto
(650) 813-5770
CLyon@mofomo.com



[Kristen J. Mathews](#)
Partner, New York
(212) 336-4038
KMathews@mofomo.com



[Julie O'Neill](#)
Partner, Boston
(617) 648-4731
JOneill@mofomo.com



[Purvi G. Patel](#)
Partner, Los Angeles
(213) 892-5296
PPatel@mofomo.com



[Nathan D. Taylor](#)
Partner, Washington, D.C.
(202) 778-1644
NDTaylor@mofomo.com



[Miriam H. Wugmeister](#)
Partner, New York
(212) 506-7213
MWugmeister@mofomo.com



The VCDPA will become **operative on January 1, 2023**. Visit [MoFo's CCPA/CPRA Resource Center](#) for additional state privacy law resources.

