VCDPA Readiness Record

The Lucid Readiness Record is a quick tool to ascertain the VCDPA maturity of your business.

This easy questionnaire is designed to start to collect information to record, measure and prioritise privacy work.

For more information on how to assess and remediate your current Privacy Program, please contact Lucid Privacy directly.

Jurisdiction[1]	
Is your organization operated for the profit or financial benefit of its shareholders or other owners?	
Does your organization conduct business in the state of Virginia or with people in Virginia?	
Does your organization collect consumers' personal data?	
Does your organisation control or process the personal data of 100,000 or more consumers in a year?	
Does your organization control or process the personal data of 25,000 consumers in a year AND derive 50% or more of its gross revenue from selling consumer personal data?	
Governance[2]	
Is there a Privacy Committee?	

[1] VCDPA § 59.1-576 (a).
[2] The provisions of this section "Governance" are not requirements under the law, but best practices in order to comply with other requirements.

Are roles and responsibilities for privacy management assigned?	
How do senior executives and leadership teams engage with matters relating to privacy and privacy risk?	
Policies	
List all relevant organisational policies relating to privacy management, eg. data protection policy, information security policy, retention policy, breach policy, etc.	
Individual Rights	
Provide details of your individual rights management processes.	
Provide details of your organisation's approach to opt outs of the sale of personal data.[3]	
Provide details of your organisation's approach to consumer opt outs of targeted advertising.[4]	
Provide details of your organisation's approach to obtain consumer opt in consent for the processing of sensitive data.[5] VCDPA defines sensitive data as: (1) precise geolocation; (2) personal data collected from a known child; (3) racial or ethnic origin; (4) religious beliefs; (5) sexual orientation; (6) citizenship or immigration status; (7) mental or physical health diagnosis; (8)	

[3] § 59.1-577 (a)(5).
[4] Id.
[5] § 59.1-578(a)(5).

genetic or biometric data for the purpose of identifying an individual.	
Provide details of your individual rights management processes relating specifically to processing data of children.[6]	
Provide details of your organisation's approach to consumers opt outs of profiling.[7]	
Provide an overview of the individual rights identity verification process.[8]	
Privacy Notice	
Provide a link to your Privacy Notice.	
Data Mapping[9]	
Do you have an inventory of personal information and associated processing?	
Do you have an information asset register?	
Training	
Provide details of your privacy training programme.[10]	

[6] § 59.1-577(a); § 59.1-57(a)(5).
[7] § 59.1-577(a)(5).
[8] § 59.1-578(e).
[9] The provisions of this section "Data Mapping" are not a requirement under the law, but a best practice in order to comply with other requirements.
[10] The VCDPA does not require employee privacy training but is a best practice in order to comply with other requirements.

Retention[11]	
Do you have in place a retention policy and retention schedule?	
Security[12]	
Do you have an information security policy?	
Describe your organisation's arrangements for managing information security and associated risks.	
Risk	
Do you have an information risk policy in place?[13]	
Do you have a privacy risk register?[14]	
How is privacy risk communicated to senior management and throughout the organisation?[15]	

[11] The provisions of this section "Retention" are not a requirement under the law, but a best practice in order to comply with other requirements.

[12] § 59.1-578(a)(3). The VCDPA requires controllers "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."

[13] This is not a requirement under the law, but a best practice in order to comply with other requirements.

[14] This is not a requirement under the law, but a best practice in order to comply with other requirements.

[15] Documenting his is not a requirement under the law, but a best practice in order to comply with other requirements.

Have you conducted data protection assessments?[16]	
Do you have a process in place for providing such data protection assessments to the Virginia attorney general upon their request?[17]	
Data Breach	
Do you have a data breach/incident response policy in place?[18]	
Vendor/Contract Management	
Do you have a policy governing processing of personal information by processors?[19]	
Have you mapped out all vendors processing personal information?[20]	
Are Data Processing Agreements/contractual terms in place with all vendors?[21]	
Do you conduct privacy specific vendor	

[16] § 59.1-580. Controllers must conduct a 'data protection assessment' when there is a heightened risk of harm to consumers, including but not limited to: (1) Targeted advertising; (2) Sales of personal data; (3) Processing personal data for profiling which creates certain risks for consumers (including unfair or deceptive treat; unlawful disparate treatment; financial, physical, or reputational injury; and other risks); and(4) Processing sensitive data. The Virginia Attorney General may request controllers provide such data protection assessment(s).

[17] § 59.1-580(c). The Virginia Attorney General may request controllers provide such data protection assessment(s).

[18] This is not a requirement under VCDPA, but under Virginia's data breach notification statute Va. Code Ann. § 18.2-186.6.

[19] This is not a requirement under the law, but may be necessary to fulfil the requirements of contract requirements with processors (see footnote 21).

[20] This is not a requirement under the law, but may be necessary to fulfil the requirements of contract requirements with processors (see footnote 21).

[21] § 59.1-579(b).

due diligence before engaging vendors?[22]	

[22] This is not a requirement under the law, but a best practice in order to comply with other requirements.