The Connecticut Data Privacy Act (CTDPA) Readiness Record

The Lucid Readiness Record is a quick tool to ascertain the CTDPA 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? (eg; not a nonprofit)	
Does your organization conduct business in the state of Connecticut or with people or devices in Connecticut?	
Does your organization collect consumers' personal data? (any unique identifiers). If yes, please provide details.	
Does your organization control or process the personal data of 100,000 or more Connecticut consumers in a year (not including personal data for the sole purpose of completing payment transactions?)	
Does your organization control or process the personal data of 25,000 consumers in a year AND derive 25% or more of its gross revenue from selling consumer personal data? (including 3rd party advertising services monetizing website visitor data)	

[1] P.A. 22-15 § 2(1)–(2).

Exemptions: Your organization is not a Connecticut state or local governing body, is not a state institution of higher education, is not subject to GLBA or HIPAA. *note CTDPA does not apply to data subject to FERPA or FCRA, or employment data.	
Governance[2]	
Is there a Privacy (Data Governance) Committee?	
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 organizational policies relating to privacy management, eg. website privacy policy, record of processing activities, data protection policy, information security/breach policy, retention policy	
Individual Rights	
Provide details of your individual rights management processes. (eg; access/deletion/modification/opt-out). Do you provide individuals with the following rights? • right to know;	

[2] The provisions of this section "Governance" are not requirements under the law, but best practices in order to comply with other requirements.

• right to access; • right to correct; • right to delete; • right to opt out of sale; • right to opt out of targeted advertising; • right to opt in to the processing of sensitive information (detailed further below); and • right to non-discrimination for exercising these rights.	
Provide details of your organization's approach to opt outs of the 'sale' of personal data.[3] (eg; direct mail lists, not third party cookies)	
Provide details of your organization's approach to consumer opt outs of targeted advertising.[4] (eg; third party advertising cookies or social media matching)	
Provide details of your organization's ability to honor opt-out preference signals (aka; 'global privacy controls').[5]	
Provide details of your organization's approach to consumers opt outs of profiling.[6]	
Provide details of your organization's approach to obtain consumer opt in consent for the processing of sensitive data.[7] CTDPA defines sensitive data as: (1) racial or ethnic origin; (2) religious beliefs; (3) mental or physical health condition or diagnosis; (4) sex life; (5) sexual orientation; (6) citizenship or immigration status; (7) personal data from a known child; (8) precise geolocation data; and (9) genetic or biometric data for the purpose of	

[3] § 6-1-1306(1)(a)(B).
[4] § 6-1-1306(1)(a)(A).
[5] § 6-1-1306(1)(a)(IV).
[6] § (a)(5)(C).
[7] § 6(a)(4).

identifying an individual.[8]	
Provide details of your individual rights management processes relating specifically to processing data of children.[9] (if relevant)	
Provide details of your organization's approach to consumers opt outs of automated profiling that may lead to a 'significant decision'.	
Provide an overview of the individual rights identity verification process.[10]	
Privacy Notice	
Provide a link to your publicly posted Privacy Notice. Under CTDPA, "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. (2) the purpose for processing personal data; 3. (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. (4) the categories of personal data that the controller shares with third parties, if any; 5. (5) the categories of third parties, if any, with which the controller shares personal data; and 6. (6) an active electronic mail address or other online	

[8] § 1(27).
[9] § 4(b).
[10] § 6(e)(1).

mechanism that the consumer may use to contact the controller."[11] In addition, "if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing."[12] Finally, "a controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to sections 1 to 11, inclusive, of this act…"[13]	
Data Mapping[14]	
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.[15]	
Data Minimization	

[11] § 6(c).
[12] § 6(d).
[13] § 6(e)(1).
[14] 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.
[15] The CTDPA does not require employee privacy training but is a best practice in order to comply with other requirements.

Does your organization only collect personal data that is "adequate, relevant and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed"?[16]	
Secondary Use	
Does your organization only process personal data that is reasonably necessary or compatible with the purpose(s) specified in the privacy policy and not process personal data for any secondary use?[17]	
Retention[18]	
Do you have in place a classification and retention policy and retention schedule?	
Security[19]	
Do you have an information security policy?	
Describe your organization's arrangements for managing information security and associated risks	
Risk	

[16] § 6(a)(1).
[17] § 6(a)(2).
[18] The provisions of this section "Retention" are not a requirement under the law, but a best practice in order to comply with other requirements.
[19] § 6(a)(3). CTDPA requires that controllers shall "establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue."

Do you have an information risk policy in place?[20]	
Do you have a privacy risk register?[21]	
How is privacy risk communicated to senior management and throughout the organization?[22]	
Have you conducted data protection assessments for all processing that presents a heightened risk of harm to consumers, including processing personal data for targeted advertising or sales, certain types of profiling, and processing sensitive data?[23]	
Data Breach[24]	
Do you have a data breach/incident response policy in place?	

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

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

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

[23] § 8(a). "A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes: (1) The processing of personal data for the purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (B) financial, physical or reputational injury to consumers, (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or (D) other substantial injury to consumers; and (4) the processing of sensitive data." Under § 8(c), the Connecticut Attorney General may request controllers provide such data protection assessment(s).

[24] This is not a requirement under CTDPA, but under Connecticut's data breach notification statute Conn. Gen. Stat. § 36a-701b.

Vendor/Contract Management	
Do you have a policy governing processing of personal information by vendors/third parties?[25]	
Have you mapped out all vendors processing personal information?[26]	
Are Data Processing Agreements/contractual terms in place with all processors?[27]	
Do you conduct privacy specific vendor due diligence before engaging vendors?[28]	

[25] This is not a requirement under the law, but may be necessary to fulfil the requirements of contract requirements with processors (see footnote 24).
[26] This is not a requirement under the law, but may be necessary to fulfil the requirements of contract requirements with processors (see footnote 24).
[27] § 7(b).
[28] This is not a requirement under the law, but a best practice in order to comply with other requirements.