The Utah Consumer Privacy Act (UCPA) Readiness Record

The Lucid Readiness Record is a quick tool to ascertain the UCPA 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 Utah or with consumers in Utah?	
Does your organization collect consumers' personal data (including unique online identifiers)?	
Does your organization have $25 million or more in annual revenue? AND	
Does your organisation control or process the personal data of 100,000 or more UT consumers in a year? OR	
Does your organization control or process the personal data of 25,000 UT consumers in a year AND derive 50% or more of its gross revenue from selling consumer personal data?	

[1] Utah Consumer Privacy Act 13-61-102(1)-(2).

Exemptions: Your organisation is not a state institution of higher education, is not subject to GLBA or HIPAA. *note UCPA does not apply to data subject to FERPA or FCRA, or employment data.	
Governance[2]	
Is there a Privacy 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 organisational policies relating to privacy management, eg. privacy policy, internal corporate data protection policy, information security policy, retention policy, data breach response policy, etc.	
Individual Rights	
Provide details of your individual rights management processes. Do you provide individuals with the following rights? • right to know; • right to access; • right to delete; • right to opt out of sale;	

[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 opt out of targeted advertising; • right to opt out of processing of sensitive data.[3]	
Provide details of your organisation's approach to opt outs of the sale of personal data (e.g., direct mail lists).[4]	
Provide details of your organisation's approach to consumer opt outs of targeted advertising (e.g., third-party advertising cookies).[5]	
Do you provide consumers with notice and an opportunity to opt-out *prior* to the processing of sensitive data?[6] UCPA defines sensitive data as: 1. personal data that reveals: a. an individuals' racial or ethnic origin (unless the personal data are processed by a video communication services); b. an individual's religious beliefs; c. an individual's sexual orientation; d. an individual's citizenship or immigration status; or e. information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care profession; 2. the processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual; or 3. specific geolocation data.[7]	
Provide details of your individual rights management processes relating specifically to processing data of	

[3] UCPA 13-61-201.
[4] UCPA 13-61-201(4)(b).
[5] UCPA 13-61-201(4)(a).
[6] UCPA 13-61-302(3).
[7] UCPA 13-61-101(32)(a).

children.[8]	
Provide an overview of individual rights identity verification ("authentication") process.[9]	
Privacy Notice	
Provide a link to your Privacy Notice. Under UCPA, a controller shall provide consumers with a reasonably accessible and clear privacy notice that includes: 1. the categories of personal data processed by the controller; 2. the purposes for which the categories of personal data are processed; 3. how consumers may exercise a right; 4. the categories of personal data that the controllers share with third parties, if any, and; 5. the categories of third parties, if any, with whom the controller shares personal data.[10] If a controller sells a consumer's personal data to one or more third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose to the consumer the manner in which the consumer may exercise the right to opt out of the: 1. sale of the consumer's personal data; or 2. processing for targeted advertising.[11]	

[8] UCPA 13-61-102(3); UCPA 13-61-202(2); UCPA 13-61-302(3)(b).
[9] UCPA 13-61-101(5); UCPA 13-61-203(5); UCPA 13-61-303(c).
[10] UCPA 13-61-301(1)(a).
[11] UCPA 13-61-301(1)(b).

Data Mapping[12]	
Do you have an inventory of personal information and associated processing?	
Do you have an information asset register?	
Training[13]	
Provide details of your privacy training programme.	
Data Minimization[14]	
Do you have in place a retention policy and retention schedule?	
Secondary Use[15]	
Do you have in place a retention policy and retention schedule?	
Retention[16]	

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

[13] The UCPA does not require employee privacy training but is a best practice in order to comply with other requirements.

[14] The UCPA does not contain any specific data minimization requirements, however, the heading of 13-61-302 reads: "Responsibilities of controllers -- Transparency -- Purpose specification and *data minimization* -- Consent for secondary use -- Security -- Nondiscrimination -- Nonretaliation -- Nonwaiver of consumer rights [emphasis added]."

[15] The UCPA does not contain any specific language requiring consent for secondary use, however, the heading of 13-61-302 reads: "Responsibilities of controllers -- Transparency -- Purpose specification and data minimization -- *Consent for secondary use* -- Security -- Nondiscrimination -- Nonretaliation -- Nonwaiver of consumer rights [emphasis added]."

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

Do you have in place a retention policy and retention schedule?	
Security[17]	
Do you have an information security policy?	
Describe your organisation's arrangements for managing information security and associated risks.	
Risk[18]	
Do you have an information risk policy in place?	
Do you have a privacy risk register?	
How is privacy risk communicated to senior management and throughout the organisation?	
Data Breach[19]	
Do you have a data breach/incident response policy in place?	

[17] UCPA 13-61-302(2). "(a) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to: (i) protect the confidentiality and integrity of personal data; and (ii) reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data. (b) Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue."

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

[19] This is not a requirement under UCPA, but under Utah's data breach notification statute Utah Code §§ 13-41-101; 13-44-202; 13-44-301.

Vendor/Contract Management	
Do you have a policy governing processing of personal information by third parties?[20]	
Have you mapped out all vendors processing personal information?[21]	
Are Data Processing Agreements/contractual terms in place with all processors?[22]	
Do you conduct privacy specific vendor due diligence before engaging vendors?[23]	

[20] This is not a requirement under the law, but may be necessary to fulfil the requirements of contract requirements with processors.
[21] This is not a requirement under the law, but may be necessary to fulfil the requirements of contract requirements with processors.
[22] UCPA 13-61-301(2). "(a) Before a processor performs processing on behalf of a controller, the processor and controller shall enter into a contract that: (a) clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, and the parties' rights and obligations; (b) requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data; and (c) requires the processor to engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data.
[23] This is not a requirement under the law, but may be necessary to fulfil the requirements of contract requirements with processors.