California Readiness Record (CCPA/CPRA)

Last Update: Nov 18, 2022

The Lucid Readiness Record is a quick tool to ascertain the CCPA/CPRA 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 California or with people in California?	
Does your organization collect consumers' personal information?	
Did your organization have $25 million or more in gross revenue in the preceding calendar year? OR	
Does your organization buy, sell, or share the personal information of 100,000 or more consumers or households in a year?[2] OR	
Does your organization derive 50% or more of its annual revenue from selling or sharing consumers' personal information?	
Governance	

[1] CCPA § 1798.140(d).
[2] Id. CPRA amends this threshold from 50,000 to 100,000

Is there a Privacy Committee?[3]	
Are roles and responsibilities for privacy management assigned?[4]	
How do senior executives and leadership teams engage with matters relating to privacy and privacy risk?[5]	
How are privacy programs and procedures documented? (Are you prepared for an audit?)[6]	
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	

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

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

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

[6] CPRA § 1798.185(a)(15). The CPRA requires businesses to conduct annual cybersecurity audits and "regular" risk assessments if the business's "processing of consumers' personal information presents significant risk to consumers' privacy or security." To determine if processing "may result in significant risk to the security of personal information," the CPRA identifies two factors to be considered: (1) the size and complexity of the business; and (2) the nature and scope of processing activities. Businesses will need to "establish a process to ensure that audits are thorough and independent."

Provide details of your organisation's approach to DNSSMPI.[7]	
Provide details of your organisation's ability to honour opt out preference signals including the Global Privacy Control.[8]	
Provide details of your organisation's approach to "Limit the Use and Disclosure of Sensitive Personal Information"[9]	
Provide details of your individual rights management processes relating specifically to processing data of children.[10]	
Provide an overview of individual rights identity verification process.[11]	
Provide an overview of your organisations record keeping of consumer requests.[12]	

[7] CPRA § 7013. Notice of Right to Opt-Out of Sale/Sharing and the "Do Not Sell or Share My Personal Information" Link. The CPRA adds the right for Consumers to opt out of the "share" of personal information. "sharing" is defined as "communicating orally, in writing, or by electronic or other means, a consumer's personal information . . . to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration" where cross-context behavioral advertising is defined as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."

[8] CPRA § 7025. Opt-Out Preference Signals. This section requires businesses that sell or share personal information to process opt-out preference signals.

[9] CPRA § 7014. Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" link.

[10] CCPA Article 6. SPECIAL RULES REGARDING CONSUMERS UNDER 16 YEARS OF AGE.. Businesses must obtain a parent or guardians affirmative authorization prior to the selling or sharing of personal information of consumers under 13. For consumers at the ages of 13-15, CPRA requires a consumer (as opposed to a parent or guardian) to consent to the sale or share of their personal information.

[11] CCPA Article 5. VERIFICATION OF REQUESTS.

[12] CCPA § 7101. Record-Keeping. For businesses collecting large amounts of personal information shall disclose such records every calendar year.

Privacy Notice	
Provide a link to your Privacy Notice, and Cookie Notice.	
Provide a link to your notice of collection and processing of Personal Information. Is this displayed at or before the point of collection?[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]	
Retention	

[13] CPRA § 7012. Notice at Collection of Personal Information. Businesses must provide "Notice at Collection" at or before the point of collection. This Notice at Collection shall include: (1) the categories of personal information about consumers; (2) the purpose(s) for which the categories of personal information are collected and used; (3) the retention schedule of each category; (4) whether the business sells or shares the personal information with a link to opt out of such sale/share; and (5) a link to the business's privacy policy. If the business collects personal information from a consumer online, the Notice at Collection may be given by linking to the privacy policy containing the above information.

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

[15] CCPA § 7100. Training.

Do you have in place a retention policy and retention schedule?[16]	
Data Minimization	
Does your organisation have a privacy review process to determine if the personal data being collected is limited to only that which is reasonably necessary to fulfil the purpose of processing?[17]	
Secondary Use	
Does your organisation have a privacy review process to determine if the personal data is only being processed for the specified purpose(s) and not for	

[16] CPRA § 7002. retention shall be "reasonably necessary and proportionate to achieve the purpose(s) for which the information was collected." While neither CCPA nor CPRA require a retention schedule, the CPRA requires businesses conduct an analysis for "reasonably necessary and proportionate:" (Whether a business's retention of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose shall be based on the following factors: (1) the minimum personal information that is necessary to achieve the purpose(s); (2) the possible negative impacts on consumers; and (3) the existence of additional safeguards to address such possible negative impacts).

[17] CPRA § 7002. Collection shall be "reasonably necessary and proportionate to achieve the purpose(s) for which the information was collected." Whether a business's collection of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose shall be based on the following factors: (1) the minimum personal information that is necessary to achieve the purpose(s); (2) the possible negative impacts on consumers; and (3) the existence of additional safeguards to address such possible negative impacts.

any secondary use for which the consumer has not been informed?[18]	
Security[19]	
Do you have an information security policy?[20]	
Describe your organisation's arrangements for managing information security and associated risks.[21]	
Have you performed a cybersecurity audit[22]	
Risk	

[18] CPRA § 7002. Restrictions on the Collection and Use of Personal Information. (c) "Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following factors: (1) At the time of collection of the personal information, the consumer's reasonable expectations concerning the purpose for which the personal information will be collected or processed, based on the factors set forth in subsection (b); (2) The other disclosed purpose for which the business seeks to further collect or process the consumer's personal information, including whether it is a Business Purpose...; (3) The strength of the link between subsection (c)(1) and subsection (c)(2). For example, a strong link exists between the consumer's expectations that the personal information will be used to provide them with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the consumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service."

[19] CPRA § 17898.150. In addition to the private right of action for breaches of non-encrypted, non-redacted personal information under the CCPA, the CPRA adds a private right of action for unauthorized access or disclosure of an email address and password or security question that would permit access to an account if the business failed to maintain reasonable security.

[20] This is not a requirement under the law, but may be deemed part of "reasonable security provisions (see footnote 21).

[21] CCPA§ 1798.100(e). "A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5."

[22] CPRA 1798.185(a)(15)(A).

Do you have an information risk policy in place?[23]	
Do you have a privacy risk register?[24]	
How is privacy risk communicated to senior management and throughout the organisation?[25]	
Have you conducted privacy risk assessments?[26]	
Do you have a process in place to submit privacy risk assessments to the state?[27]	
Data Breach	
Do you have a data breach/incident response policy in place?[28]	
Vendor/Contract Management	
Do you have a policy governing processing of personal information by third parties?[29]	

[23] This is not a requirement under the law, but may be necessary to fulfil the requirements of privacy risk assessments (see footnotes 26 and 27).
[24] This is not a requirement under the law, but a best practice in order to comply with other requirements.
[25] This is not a requirement under the law, but a best practice in order to comply with other requirements.
[26] CPRA § 1798.185(a)(15)(B).
[27] CPRA § 1798.185(a)(15)(B).
[28] This is not a requirement under the law, but a best practice in order to comply with other requirements and with California's data breach notification laws. It should be noted that the CPRA expands consumers' private right of action for data breaches (see footnote 19).
[29] This is not a requirement under the law, but may be necessary to fulfil the requirements of contract requirements with third parties (see footnotes 31 and 32).

Have you mapped out all vendors processing personal information?[30]	
Do you Data Processing Agreements/contractual terms designate each party as a 'Service Provider', 'Contractor', or 'Third Party'?[31] (see chart below)	
Are Data Processing Agreements/contractual terms in place with all vendors? (see chart below)[32]	
Do you conduct privacy specific vendor due diligence before engaging vendors?[33]	

	Service Provider/Contractor	**Third Party**
Definition	• Service Provider = "A person that processes personal information on behalf of a business and that receives from or on behalf of the business a consumer's personal information for a business purpose pursuant to a written contract." • Contractor = A person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract with the business. A service provider or contractor cannot	Essentially, a third party is a contracting party that is not a Service Provider or a Contractor. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor with respect to cross-contextual behavioral advertising services.

[30] This is not a requirement under the law, but a best practice in order to comply with other requirements, including but not limited to, contract requirements (see footnotes 31 and 32) and processing and forwarding consumer requests (§ 7026 requires businesses honor opt outs of sales/shares and notify all third parties to whom the business has sold or shared the consumer's personal information and direct them to comply with and further forward the request; § 7022 requires businesses to honor requests to delete and and to notify service providers, contractors, and third parties to comply and further forward the request; § 7027 requires businesses to honor a consumer's request to limit use and disclosure of sensitive personal information and notify service providers, contractors, and third parties to comply and further forward the request).

[31] § 7051. Contract Requirements for Service Providers and Contractors; § 7053. Contract Requirements for Third Parties.

[32] § 7051. Contract Requirements for Service Providers and Contractors; § 7053. Contract Requirements for Third Parties.

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

	contract with a business to provide cross-contextual behavioral advertising.	
Required language in contract	1. Prohibit the service provider or contractor from selling or sharing personal information it Collects pursuant to the written contract with the business. 2. Identify the specific Business Purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business, and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified Business Purpose(s) set forth within the contract. The Business Purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific. 3. Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any purpose other than the Business Purpose(s) specified in the contract or as otherwise permitted by the CCPA and these regulations. This section shall list the specific Business Purpose(s) identified in subsection (a)(2). 4. Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any commercial purpose other than the Business Purposes specified in the contract, unless expressly permitted by the CCPA or these regulations. 5. Prohibit the service provider or contractor from retaining, using, or disclosing the personal information	1. Identifies the limited and specified purpose(s) for which the personal information is made available to the third party. The purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific. 2. Specifies that the business is making the personal information available to the third party only for the limited and specified purposes set forth within the contract and requires the third party to use it only for those limited and specified purposes. 3. Requires the third party to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that the business makes available to the third party—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the third party to comply with a consumer's request to opt-out of sale/sharing forwarded to it by a first party business, and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5. 4. Grants the business the

	that it Collected pursuant to the written contract with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information that it Collected pursuant to the written contract with the business with personal information that it received from another source or Collected from its own interaction with the consumer, unless expressly permitted by the CCPA or these regulations. 6. Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it Collected pursuant to the written contract with the business—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor Page 57 of 72 to cooperating with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and to implement reasonable security procedures and practices appropriate to the nature of the personal information the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5. 7. Grant the business the right to take reasonable and appropriate steps to ensure that service provider or	right—with respect to the personal information that the business makes available to the third party—to take reasonable and appropriate steps to ensure that the third party uses it in a manner consistent with the business's obligations under the CCPA and these regulations. For example, the business may require the third party to attest that it treats the personal information the business made available to it in the same manner that the business is obligated to treat it under the CCPA and these regulations. 5. Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information made available to the third party. For example, the business may require the third party to provide documentation that verifies that it no longer retains or uses the personal information of consumers who have had their requests to opt-out of sale/sharing forwarded to it by the first party business. 6. Requires the third party to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

	contractor uses the personal information that it Collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months. 8. Require the service provider or contractor to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations. 9. Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider or contractor's unauthorized use of personal information. For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business. 10. Require the service provider or contractor to enable the business to comply with consumer requests made pursuant to the CCPA or require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with and provide the information necessary for the service provider or contractor to comply with the request.	