Pan-US Readiness Record

February, 2024 (v2.0)

The Lucid Readiness Record is a quick tool to ascertain the maturity of your business as it relates to compliance with US state privacy laws, namely the California Consumer Privacy Act as amended by the California Privacy Rights Act (collectively, the "CCPA"), the Virginia Consumer Data Protection Act ("VCDPA"), Colorado Privacy Act ("CPA"), Connecticut Data Privacy Act ("CTDPA"), the Utah Consumer Privacy Act ("UCPA"), the Oregon Consumer Privacy Act ("OCPA"), Texas Data Privacy and Security Act ("TXDPSA"), and the Montana Consumer Data Privacy Act ("MTCDPA"). This Readiness Record only covers finalized text and rulemaking as of the date of this readiness record.

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

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

Jurisdiction								
Referencing the table below, which state privacy laws apply to your organization?								
	CCPA	**VCDPA**	**CPA**	**CTDPA**	**UCPA**	**OCPA**	**TXDPSA**	**MTCDPA**
Jurisdictional Thresholds	□ Do you conduct business in CA or engage with consumers in CA? If yes: □ Did your organization	□ Do you conduct business in VA or with consumers in VA? If yes, do you: □ Control or process the personal	□ Do you conduct business in CO or with consumers in CO? If yes, do you: □ Control or process the personal	□ Do you conduct business in CT or with consumers in CT? If yes, do you: □ Control or process the personal	□ Do you conduct business in UT or with consumers in UT? If yes, do you: □ Have $25 million or more in	□ Do you conduct business in OR or with consumers in OR? If yes, do you: □ Control or process the personal	□ Do you conduct business in TX or produce products or services consumed by TX residents?	□ Do you conduct business in MT or with consumers in MT? If yes, do you: □ Control or process the personal

	have $25 million or more in total gross revenue in the preceding calendar year? **OR** □ Buy, sell, **or share**[1] the personal information of 100,000 or more CA consumers or households in a year? **OR** □ Derive 50% or more of its annual revenue from selling **or sharing** consumers' personal information *(Not just CA revenue)?*[2]	data of 100,000 or more VA consumers in a year? **OR** □ 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 (Not just VA revenue)?[3]	data of 100,000 or more CO consumers in a year? **OR** □ Derive revenue from the sale of personal data and control or process the personal data of at least 25,000 CO consumers?[4]	data of 100,000 or more CT consumers **OR** □ Control or process the personal data of 25,000 CT consumers in a year **AND** □ Derive 25% or more of its gross revenue from the sale of personal data *(Not just CT revenue)?*[5]	annual revenue? **AND EITHER:** □ Control or process the personal data of 100,000 or more UT consumers in a year? **OR** □ Control or process the personal data of 25,000 UT consumers in a year **AND** □ Derive 50% or more of its gross revenue from the sale of personal data *(Not*	data of 100,000 or more OR consumers in a year **OR** □ Control or process the personal data of 25,000 OR consumers in a year **AND** □ Derive 25% or more of its gross revenue from the sale of personal data *(Not just OR revenue)?*[7]	□ process or engage in the sale of personal data; **AND** □ You are not "small businesses" as defined by the U.S. Small Business Administration.[8][9]	data of 50,000 or more MT consumers in a year **OR** □ Control or process the personal data of 25,000 MT consumers in a year **AND** □ Derive 25% or more of its gross revenue from the sale of personal data?[10]

					just UT revenue)?[6]			

Exemptions

Referencing the table below, does your organization fall into any exemptions from these state privacy laws *(see table below)*?	

Exemption	CCPA[11]	VCDPA[12]	CPA[13]	CTDPA[14]	UCPA[15]	OCPA[16]	TXDPSA[17]	MTCDPA[18]
Non profits	Exempt	Exempt	In scope	Exempt	Exempt	In scope, however 501(c)(3)s have until July 1, 2025 to comply	Exempt	Exempt
Financial institutions and data subject to GLBA	Data subject to GLBA is exempt; the institution itself is not wholly exempt	Both exempt	Both exempt	Institutions exempt	Both exempt	Data subject to GLBA is exempt; the institution itself is not wholly exempt	Institutions exempt	Data subject to GLBA is exempt; the institution itself is not wholly exempt
Personal information subject to FCRA	Exempt	Exempt	Exempt	Exempt	Exempt	Exempts all activities subject to FCRA, and CRAs and entities that furnish data to CRAs broadly	Data subject to FCRA is exempt; the institution itself is not wholly exempt	Data subject to FCRA is exempt; the institution itself is not wholly exempt
'Covered entities'/ 'business associates' and	Limited entities exemption; Data subject to	Both exempt	Data subject to HIPAA/HITECH is exempt; the institution itself	'Covered entities'/ 'business associates'	Both exempt	Both exempt	Both exempt	Both exempt

‘protected health information’ under HIPAA and HITECH	HIPAA/HITECH is exempt; the institution itself is not wholly exempt		is not wholly exempt	exempt				
Employee/ applicant personal data within employment context	Exempt from most obligations until 1/1/2023	Exempt	Exempt	Exempt	Exempt	Exempt	Exempt	Exempt
Non-profits	Exempt	Exempt	NOT exempt	Exempt	Exempt	NOT exempt. However, 501(c)(3)s have until have until July 1, 2025, to comply	Exempt	Exempt
Institutions of higher education	Exempt if non-profit	Exempt	Exempt	Exempt	Exempt	FERPA data is exempt	Exempt	Exempt
Data Exempt from the Definition of Personal Information	● Publicly available information[19] ● De-identified data[20] ● Aggregated data[21]	● Publicly available information[22] ● De-identified data[23]	● Publicly available information[24] ● De-identified data[25]	● Publicly available information[26] ● De-identified data[27]	● Publicly available information[28] ● De-identified data[29] ● Aggregated data[30]	● Publicly available information[31] ● De-identified[32]	● Publicly available information[33] ● De-identified[34]	● Publicly available information[35] ● De-identified[36]

Governance	
Are roles and responsibilities for privacy management assigned?[37]	
How are privacy programs and procedures documented (*Are you prepared for a client/customer/other contracting party to audit your organization's privacy practices)?*[38]	
Policies	
Please list all relevant organizational 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	
Is your data subject rights (DSR) response and fulfilment process partially or fully automated? If yes, was the automation done in-house or do you use a privacy-tech vendor? *(Please specify which vendor).*	
Provide details of your individual rights management policies and processes.	
Provide details of your organization's approach to opt outs and opt ins: ● Opt out of 'sale'; ● Opt out of 'share'/targeted advertising; ● Opt out of profiling *(if relevant)*	

Provide details of your organization's approach to sensitive information. ● CCPA/CPRA, UCPA: *opt out*, (called 'limit the use and disclosure of sensitive information' under CCPA). ● VCDPA, CPA, CTDPA, OCPA, TXDPSA, MTCDPA: *opt in* to use of sensitive data The definition of sensitive information varies by jurisdiction *(see table below)*.	
Provide details of your organization's efforts to honor universal opt-out preference signals (e.g., "Global Privacy Control') . ● CCPA: effective July 2023 ● VCDPA: no requirement ● CPA: AG to release list of approved universal opt out mechanisms April 1, 2024; enforceable July 1, 2024.[39] ● CTDPA: Partial effect July 1, 2023, full effect July 1, 2025[40] ● UCPA: no requirement ● OCPA: effective July 1, 2026[41] ● TXDPSA: effective January 1, 2025[42] ● MTCPA: effective January 1, 2025[43]	
Provide details of your individual rights management processes relating specifically to processing data of children *(<13, <16 or others based on law or self-regulation)*.[44] Answer 'not applicable' if you exclude collecting data from individuals under 16.	
Provide an overview of your individual rights identity verification process *(e.g., do you require a government-issued ID for access or deletion requests)*.[45]	
Provide details of how you manage privacy requests submitted by	

authorized agents (not recognized by VCDPA or UCPA).[46]	
Do you offer consumers who have submitted a privacy rights request an appeals process for any requests your organization denied?[47] *(There is no right to appeal under CCPA or UCPA).*	
Consumer Rights Afforded by Each State	● Know / Transparency ● Access ● Delete (limited to data obtained from the consumer) ● Opt out of sale ● Opt out of 'share' / targeted advertising ● Opt out of profiling ● Non-discrimination *(Note that California splits the right of Access. Consumers may request a summary of processing and affected data categories or a full accounting of the specific data processed and the context around such uses.)*

	CCPA	**VCDPA[48]**	**CPA[49]**	**CTDPA[50]**	**UCPA[51]**	**OCPA[52]**	**TXDPSA[53]**	**MTCDPA[54]**
Additional State-Specific Consumer Rights	● Correct ● Opt out of profiling ● Opt out of the processing	● Correct ● Opt out of profiling ● Opt in to the processing of sensitive	● Correct ● Opt out of profiling ● Opt in to the processing of sensitive	● Correct ● Opt out of profiling ● Opt in to the processing of sensitive	● Opt out of the processing of sensitive personal information Must provide 1+	● Correct ● Opt out of profiling ● Opt in to the processing of sensitive	● Correct ● Opt out of profiling ● Opt in to the processing of sensitive	● Correct ● Opt out of profiling ● Opt in to the processing of sensitive

	of sensitive personal information ("Limit the Use of my sensitive personal information") ● Appeal a denial Must provide 2+ methods to exercise rights	personal information ● Appeal a denial Must provide 1+ method to exercise rights	personal information ● Appeal a denial Must provide 1+ method to exercise rights	personal information ● Appeal a denial Must provide 1+ method to exercise rights	method to exercise rights	personal information ● Appeal a denial Must provide 1+ method to exercise rights	personal information ● Appeal a denial Must provide 2+ methods to exercise rights	personal information ● Appeal a denial Must provide 1+ method to exercise rights

Definition of Sensitive Information	(1) SSN;
	(2) drivers license;
	(3) state ID;
	(4) passport/passport number;
	(5) account login information, financial account, debit card, or credit card in combination with any required security
		(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;
			(1) personal data collected from a known child;
			(2) racial or ethnic origin;
			(3) religious beliefs;
			(4) sexual orientation;
			(5) information regarding an individual's sex life;
				(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;
					(1) racial or ethnic origin;
					(2) religious beliefs;
					(3) sexual orientation;
					(4) citizenship or immigration status;
					(5) medical history, mental or physical health, medical treatment or diagnosis by a healthcare
						(1) racial or ethnic origin, national origin;
						(2) religious beliefs;
						(3) mental or physical condition or diagnosis;
						(4) sexual orientation, status as transgender or nonbinary;
						(5) status as a victim of a crime;
							(1) racial or ethnic origin;
							(2) religious beliefs;
							(3) mental or physical health diagnosis;
							(4) sexuality;
							(5) citizenship or immigration status;
							(6) genetic or biometric data processed for the purpose of
								(1) racial or ethnic origin;
								(2) religious beliefs;
								(3) mental or physical health condition or diagnosis;
								(4) information about a person's sex life or sexual orientation;
								(5) citizenship or immigration status;

	or access code, password, or credentials allowing access;
	(6) precise geolocation;
	(7) racial or ethnic origin;
	(8) religious or philosophical beliefs;
	(9) union membership;
	(10) contents of consumers mail, email, and text messages unless sent to the Business;
	(11) personal information regarding sex life or sexual orientation; and
	(12) genetic data, biometric information used for identifying the individual, and personal information
		(7) mental or physical health diagnosis;
		(8) genetic or biometric data for the purpose of identifying an individual.[56]
			(6) citizenship or immigration status;
			(7) mental or physical health diagnosis and conditions;
			(8) genetic or biometric data for the purpose of identifying an individual.[57]
				(7) personal data from a known child;
				(8) precise geolocation data; and
				(9) genetic or biometric data for the purpose of identifying an individual.[58]
					professional;
					(6) specific geolocation data;
					(7) and certain genetic personal data or biometric data, all subject to limited exceptions.[59]
						(6) citizenship or immigration status;
						(7) children's data;
						(8) precise geolocation;
						(9) genetic or biometric data.
						Sensitive Data does not include content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.[60]
							identifying an individual;
							(7) children's data; and
							(8) precise geolocation.[61]
								(6) genetic or biometric data processed for the purpose of identifying an individual;
								(7) children's data; and (8) precise geolocation.[62]

	collected and analyzed concerning a consumer's health.[55]								
Consent required for Sensitive Information	Opt out (with the right to "limit use and disclosure of sensitive information")[63]	Opt in[64]	Opt in[65]	Opt in[66]	Opt out[67]	Opt in[68]	Opt in[69]	Opt in[70]

Privacy Notice

Provide a link to your Privacy Notice (and state=specific privacy notice if applicable).	
Does your privacy notice include the following: □ The categories of personal data processed by the controller; □ The purpose for processing; □ A description of a consumer's rights; □ How consumers may exercise their rights including how a consumer may appeal; (no right to appeal in UT). Generally, organizations must provide one or more methods to exercise such rights (California and Texas require two or more methods); □ The categories of personal data shared with third parties;	

(explicitly includes sensitive data in OR);

□ The categories of third parties with whom the controller shares personal data; (OR has a more detailed requirement: "The categories of third parties with which the controller shares personal data at a level of detail that enables the consumer to understand what type of entity each third party is and, to the extent possible, how each third party may process personal data");

□ The state specific requirements detailed in the table below.

	CCPA[71]	VCDPA[72]	CPA[73]	CTDPA[74]	UCPA[75]	OCPA[76]	TXDPSA[77]	MTCDPA[78]
Content of Privacy Policy	□ A list of the categories of sources from which consumers' personal information is collected; □ The categories of personal information the business has sold or shared in the preceding 12 months;	□ Disclose the sale of data or processing for targeted advertising, and how to opt out.	N/A	□ How to contact the controller; and □ Disclose the sale of data or processing for targeted advertising, and how to opt out.	□ Disclose the sale of data or processing for targeted advertising, and how to opt out.	□ How to contact the controller; □ Identifies the controller, including any business name under which the controller registered with the Secretary of State and any assumed business	□ If a controller engages in the sale of sensitive data, the controller shall include the following notice: "NOTICE: We may sell your sensitive personal data."; and □ If a controller	□ How to contact the controller.

	□ The categories of personal information the business has disclosed about consumers for a business purpose in the preceding 12 months. *(If the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business must disclose that fact.)*; and □ Retention periods or criteria used to					name that the controller uses in this state; and □ Disclose the processing of data for targeted advertising and profiling, and how to opt out.	engages in the sale of biometric data, the controller shall include the following notice: "NOTICE: We may sell your biometric personal data."	

	determine retention periods.							
If CCPA/CPRA applies to your organization, do you display a notice at collection *(for example, do you implement a cookie banner)*?[79]								
Training[80]								
Provide details of your privacy training program *(and/or security training if privacy is included).*								
Retention[81]								
Do you have in place a data retention policy and retention schedule?								
Data Minimization[82]								
Does your organization 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?								
Secondary Use[83]								

Does your organization have a privacy review process to determine if the personal data is only being processed for the specified purpose(s) and not for any secondary use for which the consumer has not been informed?	
Security	
Do you have an information security policy?[84]	
Describe your organization's arrangements for managing information security and associated risks[85]	
If you are subject to CCPA, have you performed a cybersecurity audit?[86]	
Risk	
Have you conducted privacy risk assessments *(see thresholds below)*? Please provide any risk assessments you have.	
Do you have a process in place to respond to a state request to produce your organization's privacy risk assessments[87] *(or on a 'regular basis' to the California Privacy Protection Agency)*?[88]	

	CCPA[89]	VCDPA[90]	CPA[91]	CTDPA[92]	UCPA	OCPA[93]	TXDPSA[94]	MTCDPA[95]

When Data Protection Assessments are triggered	TBD, subject to further rulemaking	A controller shall conduct and document a DPA of each of the following processing activities involving personal data: (1) The processing of personal data for purposes of targeted advertising; (2) The sale of personal data; (3) The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial,	Where there is a heightened risk of harm to a consumer. A heightened risk of harm includes: (a) Processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of: (i) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) Financial or physical injury to consumers; (iii) A physical or other intrusion upon the solitude or seclusion, or the private affairs or	Where there is a heightened risk of harm to a consumer. A heightened risk of harm includes: (a) Processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of: (i) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) Financial or physical injury to consumers; (iii) A physical or other intrusion upon the solitude or seclusion, or the private affairs or	No requirement	Where there is a heightened risk of harm to a consumer. Processing activities that present a heightened risk of harm to a consumer include: (A) Processing personal data for the purpose of targeted advertising; (B) Processing sensitive data; (C) Selling personal data; and (D) Using the personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of: (i) Unfair or deceptive	A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data: (1) The processing of personal data for purposes of targeted advertising; (2) The sale of personal data; (3) The processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of: (A) Unfair or deceptive treatment of or unlawful	Where there is a heightened risk of harm to a consumer. A heightened risk of harm to a consumer includes: (a) The processing of personal data for the purposes of targeted advertising; (b) The sale of personal data; (c) The processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of: (i) Unfair or deceptive treatment of or unlawful disparate impact

		physical, or reputational injury to consumers; (iii) 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 (iv) Other substantial injury to consumers; (4) The processing of sensitive data; and (5) Any processing activities involving personal data that present a heightened risk of harm to consumers.	concerns, of consumers if the intrusion would be offensive to a reasonable person; or (iv) Other substantial injury to consumers; (b) Selling personal data; and (c) Processing sensitive data.	concerns, of consumers if the intrusion would be offensive to a reasonable person; or (iv) Other substantial injury to consumers; (b) Selling personal data; and (c) Processing sensitive data.		treatment of, or unlawful disparate impact on, consumers; (ii) Financial, physical or reputational injury to consumers; (iii) Physical or other types of intrusion upon a consumer's solitude, seclusion or private affairs or concerns, if the intrusion would be offensive to a reasonable person; or (iv) Other substantial injury to consumers.	disparate impact on consumers; (B) Financial, physical, or reputational injury to consumers; (C) A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or (D) Other substantial injury to consumers; (4) The processing of sensitive data; and (5) Any processing activities involving personal data that present a	on consumers; (ii) Financial, physical, or reputational injury to consumers; (iii) A physical or other form of intrusion on the solitude or seclusion or the private affairs or concerns of consumers in which the intrusion would be offensive to a reasonable person; or (iv) Other substantial injury to consumers; and (d) The processing of sensitive data

							heightened risk of harm to consumers.	

Data Breach[96]	
Do you have a data breach/incident response policy in place?	
Vendor/Contract Management	
Are Data Processing Agreements/contractual terms in place with all vendors (see table below) and do these contracts designate each party as a 'Business,' 'Service Provider,' 'Contractor,' 'Third Party,' 'Controller,' and/or 'Processor'?	
Does your Data Processing Agreement include the following: ☐ Clear instructions for processing data; ☐ The nature and purpose of processing; ☐ The type of data subject to processing; ☐ The duration of processing; ☐ The rights and obligations of both parties (including (security, and subprocessing requirements);	

□ Requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data; □ Requires the processor to engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations of the processor with respect to the personal data.	

	CCPA[97]	VCDPA[98]	CPA[99]	CTDPA[100]	UCPA[101]	OCPA[102]	TXDPSA[103]	MTCDPA[104]
Contract Requirements	*(see In Focus section below)*	□ Require the processor to, at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless required by law; □ Require the processor to make available to the	□ Require the processor to, at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless required by law; □ Require the processor to make available to the	□ Require the processor to, at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless required by law; □ Require the processor to make available to the	N/A	□ Require the processor to, at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless required by law; □ Require the processor to make available to the	□ Require the processor to, at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless required by law; □ Require the processor to make available to the	□ Require the processor to, at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless required by law; □ Require the processor to make available to the

		controller, at the controller's reasonable request, all information in its possession necessary to demonstrate the processor's compliance with its obligations herein; ☐ Requires the processor to allow, and cooperate with, reasonable assessments by the controller or the controller 's designated assessor. Alternatively, the processor may arrange for a qualified and	controller all information necessary to demonstrate compliance with its obligations herein; ☐ Requires the processor to allow, and cooperate with, reasonable assessments by the controller or the controller 's designated assessor. Alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment.	controller, at the controller's reasonable request, all information in its possession necessary to demonstrate the processor's compliance with the obligations herein; ☐ Requires the processor to allow, and cooperate with, reasonable assessments by the controller or the controller 's designated assessor. Alternatively, the processor may arrange for a qualified and		controller, at the controller's request, all information the controller needs to verify that the processor has complied with all obligations herein; ☐ Requires the processor to allow, and cooperate with, reasonable assessments by the controller or the controller 's designated assessor. Alternatively, the processor may arrange for a qualified and independen	controller, at the controller's reasonable request, all information in its possession necessary to demonstrate the processor's compliance with its obligations herein; ☐ Requires the processor to allow, and cooperate with, reasonable assessments by the controller or the controller 's designated assessor.	controller, at the controller's reasonable request, all information in its possession necessary to demonstrate the processor's compliance with its obligations herein; ☐ Requires the processor to allow, and cooperate with, reasonable assessments by the controller or the controller 's designated assessor. Alternatively, the processor may arrange for a qualified and

		independent assessor to conduct an assessment.		independent assessor to conduct an assessment.		t assessor to conduct an assessment.		independent assessor to conduct an assessment.

Requirements in Focus: CCPA		
Processors and Other Parties	**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 contract with a business to provide cross-contextual behavioral advertising.	**Third Party -** 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.
Required Contractual Language	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.	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

	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 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	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 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.

	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 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.	
Self-Regulatory/Best Practices[105]		

Are you subject to marketing / advertising industry codes of conduct or commitments?	□ ANA/DMA Direct Marketing Code of Ethics □ BBB Business Partner Code of Conduct □ IAB Code of Conduct □ IAB US Multi-State Privacy Agreement □ DAA/EDAA Self-Regulatory Principles □ NAI Code of Conduct □ Other *If none or other, please explain.*
Do you participate in any cross-industry consumer privacy choice framework or cooperative?	□ IAB Transparency & Consent Framework □ DAA/EDAA YourAdChoices □ NAI Opt Out □ ANA DMAChoice □ FCC Do Not Call
Do you participate in the IAB GPP?	
If you engage in mobile, how do you obtain consent in iOS and Android? *Please provide screenshots of your ATT and Google consent.* *Please also provide any relevant details about your compliance with Apple's (e.g. ATT, Manifests) and Google's app store policies as part of your U.S. privacy strategy.*	
Are you a registered data broker?	

Have you registered in CA, OR, TX, and VT?	
Is there a Privacy Committee?	
How do senior executives and leadership teams engage with matters relating to privacy and privacy risk	
Provide a link to your cookie notice and/or cookie banner.[106]	
Do you have an inventory of all personal information attributes and associated processing activities?	
Do you have an information asset and/or classification register?	
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 organization?	
Do you have a policy governing processing of personal information by service providers/vendors/third parties?	

Have you created a data inventory map identifying all vendors processing personal information?	
Do you conduct privacy-specific vendor due diligence before engaging vendors (If privacy is included in security reviews, please specify)?	

Endnotes

1. CCPA defines 'Sharing' 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." Cross-context behavioral advertising means "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." Given this broad definition, cross-context behavioral advertising includes the use of 3rd party cookies or IP addresses for retargeting visitors through another media channel. To be clear; most ad supported websites should fall into this category if they rely on 3rd party cookies.
2. CCPA § 1798.140(d). Did your organization have $25 million or more in total gross revenue in the preceding calendar year is a global calculation NOT just UT revenue. Derive 50% or more of its annual revenue from selling or sharing consumers' personal information is also a global analysis NOT just CA revenue.
3. VCDPA § 59.1-576 (a).
4. CPA § 6-1-1304.
5. CTDPA § 22-15 § 2(1)–(2). Control or process the personal data of 100,000 or more CT consumers in a year does NOT include personal data for the sole purpose of completing payment transactions.
6. UCPA § 13-61-102(1)-(2). Have $25 million or more in annual revenue is global revenue, NOT just UT revenue.
7. OCPA § 2(1). Control or process the personal data of 100,000 or more OR consumers in a year does NOT include personal data for the sole purpose of completing payment transactions.
8. TXDPSA § 541.002(a).
9. Definitions of "small business" by the SBA vary widely from one industry vertical to the next.
10. MTCDPA § 3. Control or process the personal data of 50,000 or more MT consumers in a year does NOT include personal data for the sole purpose of completing payment transactions.
11. CCPA § 1798.145.
12. VCDPA § 59.1-576(c).
13. CPA § 6-1-1304(2).
14. CTDPA § 3.
15. UCPA § 13-61-102(2).
16. OCPA § 2(2).
17. TXDPSA § 541.002(b).
18. MTCDPA § 4.
19. CCPA § 1798.140(L)(2) "'Publicly available' means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge."
20. CCPA § 1798.140(m) "'Deidentified' means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer…"

Deidentification requirements: Business must: "(1) Take reasonable measures to ensure that the information cannot be associated with a consumer or household. (2) Publicly commit to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision. (3) Contractually obligate any recipients of the information to comply with all provisions of this subdivision."

21. CCPA § 1798.140(b) “‘Aggregate consumer information’ means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. “Aggregate consumer information” does not mean one or more individual consumer records that have been deidentified.”
22. VCDPA § 59.1-575. “‘Publicly available information' means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience."
23. VCDPA § 59.1-575. "'De-identified data' means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person.”

De-identification requirements: § 59.1-581(a): “The controller in possession of de-identified data shall: (1)Take reasonable measures to ensure that the data cannot be associated with a natural person; (2) Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and (3) Contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.”

24. CPA § 6-1-1303(17)(b) “‘Publicly available information’ means information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public.”
25. CPA § 6-1-1303(11) "'De-identified data’ means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual…”

De-identification requirements:, Controller must: (a) take reasonable measures to ensure that the data cannot be associated with an individual; (b) publicly commit to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data; and (c) contractually obligate any recipients of the information to comply with the requirements of this subsection (11).

26. CTDPA § 1(25) “‘Publicly available information’ means information that (A) is lawfully made available through federal, state or municipal government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.”
27. CTDPA § 1(13) "'De-identified data’ means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual…”

De-identification requirements: Controller must: (A) take reasonable measures to ensure that such data cannot be associated with an individual, (B) publicly commit to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligate any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

28. UCPA § 13-61-101(29) "'Publicly available information’ means information that (A) is lawfully made available through federal, state or municipal government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.”
29. UCPA § 13-6101(14)(a) "'Deidentified data’ means data that: (a) cannot reasonably be linked to an identified individual or an identifiable individual…”

Deidentification requirements: § 13-6101(14)(b) Controller must: (i) take reasonable measures to ensure that a person cannot associate the data with an individual; (ii) publicly commit to maintain and use the data only in deidentified form and not attempt to reidentify the data; and (iii) contractually obligate any recipients of the data to comply with the requirements described in Subsections (14)(b)(i) and (ii).

30. UCPA § 13-61-101(3) “‘Aggregated data’ means information that relates to a group or category of consumers: (a) from which individual consumer identities have been removed; and (b) that is not linked or reasonably linkable to any consumer.”
31. OCPA § 1(13). “Publicly available information” isn’t specifically defined. Rather, “‘Personal data’ does not include data that: (A) Is lawfully available through federal, state or local government records or through widely distributed media; or (B) A controller reasonably has understood to have been lawfully made available to the public by a consumer.”
32. OCPA § 1(11) Deidentified data is data that, “Cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable consumer, or to a device that identifies, is linked to or is reasonably linkable to a consumer; or (b) Is: (A) Derived from patient information that was originally created, collected, transmitted or maintained by an entity subject to regulation under the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as in effect on the effective date of this 2023 Act, or the Federal Policy for the Protection of Human Subjects, codified as 45 C.F.R. part 46 and in various other deferral regulations, as codified in various sections of the

Code of Federal Regulations and as in effect on the effective date of this 2023 Act; and (B) Deidentified as provided in 45 C.F.R. 164.514, as in effect on the effective date of this 2023 Act."

Deidentification requirements: § 7(1)(a) "A controller that possesses deidentified data shall: (A) Take reasonable measures to ensure that the deidentified data cannot be associated with an individual; (B) Publicly commit to maintaining and using deidentified data without attempting to reidentify the deidentified data; and (C) Enter into a contract with a recipient of the deidentified data and provide in the contract that the recipient must comply with the controller's obligations under sections 1 to 9 of this 2023 Act. (b) A controller that discloses deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject and shall take appropriate steps to address any breaches of the contractual commitments."

33. TXDPSA § 541.001(27). "'Publicly available information' means information that is lawfully made available through government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted the information to a specific audience."
34. TXDPSA § 541.001(12) "'Deidentified data' means data that cannot reasonably be linked to an identified or identifiable individual, or a device linked to that individual."

Deidentification requirements: § 541.106(a). "A controller in possession of deidentified data shall: (1) take reasonable measures to ensure that the data cannot be associated with an individual; (2) publicly commit to maintaining and using deidentified data without attempting to reidentify the data; and (3) contractually obligate any recipient of the deidentified data to comply with the provisions of this chapter."

35. MTCDPA § 2(22) "'Publicly available information' means information that: (a) is lawfully made available through federal, state, or municipal government records or widely distributed media; or (b) a controller has a reasonable basis to believe a consumer has lawfully made available to the public."
36. MTCDPA § 2(11). "'Deidentified data' means data that cannot be used to reasonably infer information about or otherwise be linked to an identified or identifiable individual or a device linked to the individual if the controller that possesses the data: (a) takes reasonable measures to ensure that the data cannot be associated with an individual; (b) publicly commits to process the data in a deidentified fashion only and to not attempt to reidentify the data; and (c) contractually obligates any recipients of the data to satisfy the criteria set forth in subsections (11)(a) and (11)(b)."
37. This is not a requirement under the law, but a best practice in order to comply with other requirements.
38. 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."
39. CPA § (1)(a)(IV)(A).
40. CTDPA § 6(e)(1)(A).
41. OCPA § 5(5)(c).
42. TXDPSA § 541.055(e).
43. MTCDPA § 6(3)(b).
44. CCPA § 999.330; § 1798.120(c). VCDPA, CPA, CTDPA, UCPA, OCPA, TXDPSA, and MTCDPA treat children's data as sensitive data. VCDPA § 59.1-575; § 59.1-578(A)(5); CPA § 6-1-1303(24)(c); § 6-1-1308(6); CTDPA § 1(27); § 4(b); UCPA 13-61-102(3); § 13-61-202(2); § 13-61-302(3)(b); OCPA § 1(18); § 4(3); § 5(2)(b); TXDPSA § 541.001(29)(c); § 541.005; § 541.051(a); § 541.101(b)(4); MTCDPA § 2(24(c); § 4(3) § 5(3)(b); § 7(2)(b).
45. CCPA article 4; VCDPA § 59.1-578(E); CPA § 6-1-1306(1); CTDPA § 5; UCPA § 13-61-203(5)(b); OCPA § 4(5); TXDPSA § 541.051(a); § 541.051(e); MTCDPA § 5(4)(d).
46. CCPA § 1798.185(a)(7); CPA § 6-1-1306(1)(a)(II); CTDPA § 5; OCPA § 4(4); TXDPSA § 541.055(e); MTCDPA § 5(3).
47. VCDPA § 59.1-578(c)(3); CPA § 6-1-1306(3)(A); CTDPA § (4)(d). There is no right to appeal under CCPA or VCDPA. However, under CCPA, if a Business denies a request, the Business must provide Consumers with the basis for the denial. OCPA § 4(6); TXDPSA § 541.052(c); MTCDPA § 5(4)(b); § 5(5).
48. VCDPA § 59.1-577.
49. CPA § 6-1-1306.

50. CTDPA § 4.
51. UCPA § 13-61-201.
52. OCPA § 3.
53. TXDPSA § 541.051.
54. MTCDPA § 5.
55. CCPA § 1798.130(ae).
56. VCDPA § 59.1-575; 59.1-578(A)(5).
57. CPA § 6-1-1303(24); § 6-1-1308(7).
58. CTDPA § 1(27); §6(a)(4).
59. UCPA § 13-61-101(32); § 13-61-302(3).
60. OCPA § 1(18).
61. TXDPSA § 541.001(29).
62. MTCDPA § 2(24).
63. CPRA § 7014.
64. VCDPA § 59.1-578(a)(5).
65. CPA § 6-1-1308(7).
66. CTDPA § 6(a)(4).
67. UCPA 13-61-302(3).
68. OCPA § 5(2)(b).
69. TXDPSA § 541.101(b)(4).
70. MTCDPA § 7(2)(b).
71. CCPA § 1798.140(ae); § 1798.121. Note, the two or more designated methods for submitting requests, must include, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests. In addition, a business that maintains a website must make the website available to consumers to submit requests.
72. VCDPA § 59.1-578(c)-(e).
73. CPA § 6-1-1308(a).
74. CTDPA § 6(c)-(e)(1).
75. UCPA § 13-61-301(1)(b).
76. OCPA § 5(4).
77. TXDPSA § 541.102.
78. MTCDPA § 7(5).
79. 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. IT SHOULD BE NOTED THAT A COOKIE BANNER IS NOT PRESCRIBED UNDER LAW.
80. CCPA § 7100. The CCPA requires Businesses train their employees in privacy issues. employee.
81. 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).

82. (This is a 'Privacy by Design' recommended best practice for all organizations, and is also required under the CCPA, CPA, and CTDPA).
83. 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."
84. This is not a requirement under the law, but may be helpful to comply with security requirements (see footnotes 46 & 47).
85. 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."
86. CCPA 1798.185(a)(15)(A). CCPA requires an annual cybersecurity audit that must be submitted to the CA AG. This provision is subject to future rulemaking.
87. VCDPA § 59.1-580(c); CPA § 6-1-1309(4); CTDPA § 8(c); OCPA §8(3) ; TXDPSA § 541.105(c); MTCDPA § 9(3).
88. CCPA § 1798.185(a)(15)(B). This is subject to future rulemaking.
89. CPRA § 1798.185(a)(15)(B). This provision is subject to further rulemaking.
90. VCDPA § 59.1-580. The Virginia Attorney General may request controllers provide such data protection assessment(s).
91. CPA § 6-1-1309.
92. CTDPA § 8(a).
93. OCPA § 8(1)(a)-(b).
94. TXDPSA § 541.105(a).
95. MTCDPA § 8(1).
96. This is not a requirement under these privacy laws, but a requirement under state data breach notification laws. It should be noted that the CPRA expands consumers' private right of action for data breaches by authorising consumers to bring lawsuits arising from data breaches involving additional categories of personal information. Specifically, the CPRA adds email addresses in combination with a password or security question and answer that would permit access to the consumer's account to the list of data types that can be actionable under the law in the event of a breach (CCPA § 1798.150(a)(1)).
97. CCPA § § 7051. Contract Requirements for Service Providers and Contractors; § 7053. Contract Requirements for Third Parties.
98. VCDPA § 59.1-579(B).
99. CPA § 6-1-1305(5).
100. CTDPA § 7(b).
101. UCPA § 13-61-301(2).
102. OCPA § 6(2).
103. TXDPSA §541.104(b)-(c).
104. MTCDPA § 8(2).
105. The provisions of this section are not required under law, but a best practice in order to comply with other requirements.

106. It should be noted that cookie banners are not prescribed under law and often are in conflict with the consent requirements under these state privacy laws.