Pan-US Readiness Record

March, 2023

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 ("CCPA") and its amendments including the California Privacy Rights Act ("CPRA"), the Virginia Consumer Data Protection Act ("VCDPA"), Colorado Privacy Act ("CPA"), Connecticut Data Privacy Act ("CTDPA"), and the Utah Consumer Privacy Act ("UCPA"). This Readiness Record only covers finalized text and rulemaking as of the date of this readiness record. For the sake of clarity, this readiness record does not cover the CCPA rulemaking process that commenced July 8, 2022 or the CPA draft regulations released September 30, 2022. This readiness record and the legal requirements herein are subject to the finalization of the CCPA rulemaking (which has been submitted to the OAL for final approval) and the CPA rulemaking.

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

CCPA/CPRA	VCDPA	CPA	CTDPA	UCPA
☐ Is your organization for-profit? ☐ Does your organization conduct business in the state of California or engage with California consumers?	☐ Is your organization for-profit? ☐ Does your organization conduct business in the state of Virginia or with people in Virginia? If the answer to the above questions is yes:	☐ Does your organization conduct business in the state of Colorado or with people in Colorado? If yes: ☐ Does your organization control or process the	☐ Is your organization for-profit? ☐ Does your organization conduct business in the state of Connecticut or with people in Connecticut?	☐ Is your organization for-profit? ☐ Does your organization conduct business in the state of Utah or with people in Utah? If the answer to the above questions is yes:

If the answer to the above questions is yes: ☐ Did your organization have $25 million or more in total (not just CA) gross revenue in the preceding calendar year? OR ☐ Does your organization buy, sell, **or share**[1] the personal information of 100,000 or more CA consumers or households in a year? OR ☐ Does your organization derive 50% or more of its annual revenue from selling **or sharing** consumers' personal	☐ Does your organization control or process the personal data of 100,000 or more VA consumers in a year? OR ☐ Does your organization control or process the personal data of 25,000 consumers in a year AND derive 50% or more of its gross revenue from selling consumer personal data (Not just VA revenue)?[3]	personal data of 100,000 or more CO consumers in a year? OR ☐ Does your organization derive revenue from the sale of personal data and control or process the personal data of at least 25,000 CO consumers?[4]	If the answer to the above questions is yes: ☐ Does your organization control or process the personal data of 100,000 or more CT consumers in a year (not including personal data for the sole purpose of completing payment transactions? OR ☐ Does your organization 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	☐ Does your organization have $25 million or more in annual revenue? (*Not just UT revenue.)* and EITHER: ☐ 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

[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.

[3] VCDPA § 59.1-576 (a).

[4] CPA § 6-1-1304.

information (Not just CA revenue)?[2]			data (Not just CT revenue)?[5]	gross revenue from the sale of personal data (Not just UT revenue)?[6]

Exemptions

Does your organization fall into any exemptions from these state privacy laws (see table below)?

Exemption	CCPR/CPRA[7]	VCDPA[8]	CPA[9]	CTDPA[10]	UCPA[11]
Financial institutions and data subject to GLBA	Institutions not exempt; data exempt	Both exempt	Both exempt	Institutions exempt	Both exempt
'Covered entities'/ 'business associates' and 'protected health information' under	Limited entities exemption; data exempt	Both exempt	Data exempt	'Covered entities'/ 'business associates' exempt	Both exempt

[2] CCPA § 1798.140(d).
[5] CTDPA § 22-15 § 2(1)–(2).
[6] UCPA § 13-61-102(1)-(2).
[7] CCPA § 1798.145.
[8] VCDPA § 59.1-576(c).
[9] CPA § 6-1-1304(2).
[10] CTDPA § 3.
[11] UCPA § 13-61-102(2).

HIPAA and HITECH					
Personal information subject to FCRA	Exempt	Exempt	Exempt	Exempt	Exempt
Employee/ applicant personal data within employment context	Exempt from most obligations until 1/1/2023	Exempt	Exempt	Exempt	Exempt
Non-profits	Exempt	Exempt	Not exempt	Exempt	Exempt
Institutions of higher education	Exempt if non-profit	Exempt	Exempt	Exempt	Exempt
Data Exempt from the Definition of	• Publicly available	• Publicly available	• Publicly available	• Publicly available	• Publicly available

Personal Information	information[12] • De-identified	information[15] • De-identified	information [17] • De-identified	information[19] • De-identified	information[21] • De-identified

[12] 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."

[15] 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."

[17] 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."

[19] 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."

[21] 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."

	• data[13] • Aggregated data[14]	data[16]	data[18]	data[20]	• data[22] • Aggregated data[23]

Governance	
Are roles and responsibilities for privacy	

[13] CCPA § 1798.140(m) "'Deidentified' means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information: (1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household. (2) Publicly commits 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 obligates any recipients of the information to comply with all provisions of this subdivision."

[14] 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."

[16] 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. A controller that possesses "de-identified data" shall comply with the requirements of subsection A of § 59.1-581."

[18] 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, 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 maintain and use the data only in a de-identified fashion and not attempt to re-identify the data; and (c) contractually obligates any recipients of the information to comply with the requirements of this subsection (11).

[20] 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, if the controller that possesses such data (A) takes reasonable measures to ensure that such data cannot be associated with an individual, (B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision."

[22] UCPA § 13-6101(14) "Deidentified data" means data that: (a) cannot reasonably be linked to an identified individual or an identifiable individual; and (b) are possessed by a controller who: (i) takes reasonable measures to ensure that a person cannot associate the data with an individual; (ii) publicly commits to maintain and use the data only in deidentified form and not attempt to reidentify the data; and (iii) contractually obligates any recipients of the data to comply with the requirements described in Subsections (14)(b)(i) and (ii)."

[23] 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."

management assigned?[24]	
How are privacy programs and procedures documented (Are you prepared for a client/customer/other contracting party to audit your organization's privacy practices)?[25]	

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).*	

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

[25] 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 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: '*limit the use and disclosure of sensitive information*' ● VCDPA, CPA, CTDPA: *opt in* to use of sensitive data ● UCPA: *opt out* 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).[26] ● VCDPA: no requirement ● CPA: AG to release list of approved universal opt out mechanisms April	

[26] CCPA rulemaking proposed final text https://cppa.ca.gov/meetings/materials/20230203_item4_text.pdf.

1, 2024; enforceable July 1, 2024.[27] • CTDPA: Partial effect July 1, 2023, full effect July 1, 2025[28] • UCPA: no requirement	
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).[29] 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).[30]	
Provide details of how you manage privacy requests submitted by authorized agents (not recognized by VCDPA or UCPA).[31]	
Do you offer consumers who have submitted a privacy rights request an appeals process for any requests your organization denied?[32]	

[27] CPA § (1)(a)(IV)(A).
[28] CTDPA § 6(e)(1)(A).
[29] CCPA § 999.330; § 1798.120(c). VCDPA, CPA, CTDPA, and UCPA 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).
[30] CCPA article 4; VCDPA § 59.1-578(E); CPA § 6-1-1306(1); CTDPA § 5; UCPA § 13-61-203(5)(b).
[31] CCPA § 1798.185(a)(7); CPA § 6-1-1306(1)(a)(II); CTDPA § 5.
[32] 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.

(There is no right to appeal under CCPA or UCPA).	

	CCPA/CPRA	VCDPA	CPA	CTDPA	UCPA
Consumer Rights	• Know • Access • Correction • Deletion (limited to data obtained from the consumer) • Opt out of sale • Opt out of share of their personal information • Opt out of the processing of sensitive personal information (called "Limit the Use of my sensitive personal	• Know • Access • Correction • Deletion • Opt out of sale • Opt out of targeted advertising • Opt in to the processing of sensitive personal information • Non-discrimination[33]	• Know • Access • Correction • Deletion • Opt out of sale • Opt out of targeted advertising • Opt in to the processing of sensitive personal information • Non-discrimination[34]	• Know • Access • Correction • Deletion • Opt out of sale • Opt out of targeted advertising • Opt in to the processing of sensitive personal information • Non-discrimination[35]	• Know • Access • Deletion (limited to data obtained from the consumer) • Opt out of sale • Opt out of share targeted advertising • Opt out of the processing of sensitive personal information • Non-discrimination[36]

[33] VCDPA § 59.1-577.
[34] CPA § 6-1-1306.
[35] CTDPA § 4.
[36] UCPA § 13-61-201.

	information") • Non-discrimination				
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 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,	(1) precise geolocation; (2) personal data collected from a known child; (3) racial or ethnic origin; (4) religious beliefs; (5) sexual orientation; (6) citizenship or immigration status; (7) mental or physical health diagnosis; (8) genetic or biometric data for the purpose of identifying an individual.[38]	(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; (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.[39]	(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 identifying an individual.[40]	personal data that reveals an individual's (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 professional; (6) specific geolocation data; (7) and certain genetic personal data or biometric data, all subject to limited exceptions.[41]

[38] VCDPA § 59.1-575; 59.1-578(A)(5).
[39] CPA § 6-1-1303(24); § 6-1-1308(7).
[40] CTDPA § 1(27); §6(a)(4).
[41] UCPA § 13-61-101(32); § 13-61-302(3).

	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 collected and analyzed concerning a consumer's health.[37]				
Consent required for Sensitive Information	Opt out (with the right to "limit use and disclosure of sensitive information")[42]	Opt in[43]	Opt in[44]	Opt in[45]	Opt out[46]

[37] CCPA § 1798.130(ae).
[42] CPRA § 7014.
[43] VCDPA § 59.1-578(a)(5).
[44] CPA § 6-1-1308(7).
[45] CTDPA § 6(a)(4).
[46] UCPA 13-61-302(3).

Privacy Notice

Provide a link to your Privacy Notice (and state=specific privacy notice if applicable).				
Does your privacy notice include the following:				
CCPA/CPRA[47]	**VCDPA[48]**	**CPA[49]**	**CTDPA[50]**	**UCPA[51]**
☐ A description of a consumer's rights ☐ Two or more designated methods for submitting requests, including, at a minimum, a toll-free telephone number. (Note: A business that operates exclusively online and has a direct relationship with a consumer from	Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes: ☐ The categories of personal data processed by the controller; ☐ The purpose for processing personal data;	☐ The categories of personal data collected or processed by the controller or a processor; ☐ The purposes for which the categories of personal data are processed; ☐ How and where consumers may exercise the rights including the	"A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes: ☐ The categories of personal data processed by the controller; ☐ The purpose for processing personal data; ☐ How consumers may	A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes: ☐ The categories of personal data processed by the controller; ☐ The purposes for which the categories of personal data are processed; ☐ How consumers may

[47] CCPA § 1798.140(ae); § 1798.121.
[48] VCDPA § 59.1-578(c)-(e).
[49] CPA § 6-1-1308(a).
[50] CTDPA § 6(c)-(e)(1).
[51] UCPA § 13-61-301(1)(b).

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. ☐ A list of the categories of personal information a business has collected about consumers in the preceding 12 months; ☐ A list of the categories of sources from which consumers' personal information is collected; ☐ The business or commercial purpose for collecting or selling or sharing consumers' personal information;	☐ How consumers may exercise their consumer rights pursuant § 59.1-577, including how a consumer may appeal a controller's decision with regard to the consumer's request; ☐ The categories of personal data that the controller shares with third parties, if any; and ☐ The categories of third parties, if any, with whom the controller shares personal data. ☐ 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	controller's contact information and how a consumer may appeal a controller's action with regard to the consumer's request; ☐ The categories of personal data that the controller shares with third parties, if any; and ☑ The categories of third parties, if any, with whom the controller shares personal data.	exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; ☐ The categories of personal data that the controller shares with third parties, if any; ☐ The categories of third parties, if any, with which the controller shares personal data; and ☐ An active electronic mail address or other online mechanism that the consumer may use to contact the controller." ☐ If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such	exercise a right; ☐ The categories of personal data that the controllers share with third parties, if any, and; ☐ The categories of third parties, if any, with whom the controller shares personal data. ☐ If a controller sells a consumer's personal data to one or more third parties, 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 sale of personal data. ☐ If a controller engages in targeted advertising, the controller shall clearly and conspicuously disclose to the consumer the

☐ The categories of third parties to whom the business discloses consumers' personal information; and ☐ A list of the categories of personal information the business has sold or shared about consumers in the preceding 12 months; and ☐ A list of the categories of personal information the business has disclosed about consumers for a business purpose in the preceding 12 months. Note: if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business must disclose that fact.	opt out of such processing. ☐ 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 under this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to § 59.1-577 but may		processing, as well as the manner in which a consumer may exercise the right to opt out of such processing. ☐ 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.	manner in which the consumer may exercise the right to opt out of the processing for targeted advertising.

	require a consumer to use an existing account.			
If CCPA/CPRA applies to your organization, do you display a notice at collection (for example, do you implement a cookie banner)??[52]				
Training[53]				
Provide details of your privacy training program (and/or security training if privacy is included).				
Retention[54]				
Do you have in place a data retention policy and retention schedule?				

[52] 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..

[53] CCPA § 7100. The CCPA requires Businesses train their employees in privacy issues. employee
The provisions of this section "Training" are not requirements under the VCDPA, CPA, CTDPA, and CPA, but best practices in order to comply with other requirements.

[54] 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).
The provisions of this section "Retention" are not requirements under the VCDPA, CPA, CTDPA, and CPA, but best practices in order to comply with other requirements.

Data Minimization[55]	
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?	

[55] (This is a 'Privacy by Design' recommended best practice for all organizations, and is also required under the CCPA, CPA, and CTDPA).
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.
The VCDPA does not contain any data minimization provisions.
CPA § 6-1-1308(3).
CTDPA § 6(a)(1).
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 -- Non Retaliation -- Non Waiver of consumer rights [emphasis added]."

Secondary Use[56]	
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?[57]	
Describe your organization's arrangements for	

[56] 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."
The VCDPA does not contain any secondary use provisions.
CPA § 6-1-1308(4).
CTDPA § 6(a)(2).
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 -- Non Retaliation -- Non Waiver of consumer rights [emphasis added]."
[57] This is not a requirement under the law, but may be helpful to comply with security requirements (see footnotes 46 & 47).

managing information security and associated risks[58]	
If you are subject to CCPA, have you performed a cybersecurity audit?[59]	
Risk	
Have you conducted privacy risk assessments? • CCPA/CPRA[60] • VCDPA: 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, where such profiling presents a	

[58] 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."
VCDPA § 59.1-578(a)(3). The VCDPA requires controllers " Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue."
CPA § 6-1-1305(4). CPA requires, "Taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement the measures."
CTDPA § 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."
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."
[59] 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.
[60] CPRA § 1798.185(a)(15)(B). This provision is subject to further rulemaking.

reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, 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.[61] • CPA, CTDPA: A Controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting a data protection assessment. 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 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.[62][63]	

[61] VCDPA § 59.1-580. The Virginia Attorney General may request controllers provide such data protection assessment(s).
[62] CPA § 6-1-1309.
[63] CTDPA § 8(a).

• UCPA: no requirement.	
Do you have a process in place to respond to a state request to produce your organization's privacy risk assessments[64] (or on a 'regular basis' to the California Privacy Protection Agency)?[65]	
Data Breach[66]	
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'?[67]	

[64] VCDPA § 59.1-580(c); CPA § 6-1-1309(4); CTDPA § 8(c).
[65] CCPA § 1798.185(a)(15)(B). This is subject to future rulemaking.
[66] 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)).
[67] CCPA § 7051. Contract Requirements for Service Providers and Contractors; § 7053. Contract Requirements for Third Parties; VCDPA § 59.1-579(b); CPA 6-1-1305((5); CTDPA § 7(b); UCPA 13-61-301(2).

	CCPA/ CPRA[68]	VCDPA[69]	CPA[70]	CTDPA[71]	UCPA[72]
Contract Requirements	(see below)	A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall: 1. Ensure that each person processing personal data is subject to a duty of	Processing by a processor must be governed by a contract between the controller and the processor that is binding on both parties and that sets out: (a) The processing instructions to which the processor is bound, including the nature and purpose of the processing; (b) The type of personal data subject to the processing, and the duration of the processing; (c) The requirements imposed by this subsection (5) and subsections (3) (confidentiality and subprocessing requirements) and (4) (security) of this section; and (d) The following requirements: (i) At the	A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that the processor: (1) Ensure that each person processing personal data is subject to a duty of confidentiality with	(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

[68] CCPA § § 7051. Contract Requirements for Service Providers and Contractors; § 7053. Contract Requirements for Third Parties.
[69] VCDPA § 59.1-579(B).
[70] CPA § 6-1-1305(5).
[71] CTDPA § 7(b).
[72] UCPA § 13-61-301(2).

		confidentiality with respect to the data; 2. 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 retention of the personal data is required by law; 3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter; 4. 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 of the processor's policies and technical and organizational	choice of the controller, the processor shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (ii) (a) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this part 13; and (b) The processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit of the processor's policies and technical and organizational	respect to the data; (2) 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 retention of the personal data is required by law; (3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 1 to 11, inclusive, of this act; (4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and (5) allow, and cooperate with, reasonable assessments by the	subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data.

		measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and 5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data.	measures in support of the obligations under this part 13 using an appropriate and accepted control standard or framework and audit procedure for the audits as applicable. the processor shall provide a report of the audit to the controller upon request.	controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 1 to 11, inclusive, of this act, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.	

CCPA	Service Provider/Contractor	Third Party
CCPA definitions	**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."	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

	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.	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. 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	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

	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 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	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.

	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[73]	
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.[74]	
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?	

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

[74] 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.

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)?	