	Timing	Content	Storage	Updates	Government Access
VCDPA	Required for processing activities conducted or generated after January 1, 2023, and when: - Processing for targeted advertising, - Selling personal data - Processing for profiling that presents certain risks, - Processing sensitive data, - Other processing activities involving a heightened risk of harm to consumers.	Identify and weigh the benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against potential risks to the rights of the consumer associated with such processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of consumers, the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed.	N/A	N/A	Controllers must disclose a DPIA to the Virginia AG upon request. DPIAs will be confidential and exempt from disclosure.
CPA	Required for processing activities conducted or generated after July 1, 2023, and before initiating certain activities, including: - Sale of personal data, - Processing sensitive data, - Processing for targeted advertising, - Processing for profiling that presents certain risks, - other substantial injury to consumers.	Identify and describe the risks to the rights of consumers associated with the processing, document measures considered and taken to address and offset those risks, contemplate the benefits of the processing, and demonstrate that the benefits of the processing outweigh the risks offset by safeguards in place. The CPA Regs also require 12 specific pieces of information, including an additional 12 if profiling.	DPIAs must be stored for as long as the processing activity continues, and for at least three (3) years after it has concluded.	Review and update DPIA as often as appropriate considering type, amount, sensitivity of data, and level of risk. If profiling, review and update DPIA at least annually.	Controllers must disclose a DPIA to the Colorado AG within 30 days of the AG's request. The DPIA will be confidential and exempt from disclosure.
CTPA	Required for processing activities conducted or generated after July 1, 2023, and when: - Processing for targeted advertising, - Selling personal data - Processing for profiling that presents certain risks, - Processing sensitive data, - Other processing activities involving a heightened risk of harm to consumers.	Identify and weigh the benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against potential risks to the rights of the consumer associated with such processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of consumers, the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed.	N/A	N/A	Controllers must disclose a DPIA to the Connecticut AG upon request. The DPIA will remain confidential and exempt from disclosure.

	Timing	Content	Storage	Updates	Government Access
CCPA	TBD, but potentially everything required by CPA plus regarding "sharing" of personal information and the following that come from the EDPB Guidelines the CPPA has stated that they are looking to in addition to the CPA Regs: Required prior to processing that is likely to result in a high risk to rights and freedoms, including for: - Profiling, - Automated decision-making, - Systemic monitoring and processing of consumers in a publicly accessible area, - Processing sensitive data, - Processing data on a large scale, - Matching or combining data sets - Data concerning vulnerable consumers, - Innovative use or new technology - When processing itself prevents consumers from exercising a right or using a service.	TBD, but potentially everything required by CPA and the following that come from the EDPB Guidelines the CPPA has stated that they are looking to in addition to the CPA Regs: At a minimum, DPIAs must contain the following information: - A description of the Processing activity; - Purposes of the processing; - An assessment of necessity and proportionality; - A detailed assessment of risks; - A description of the measures to address the risks; and - The involvement of all interested parties, where appropriate.	TBD. N/A under EDPB, but applicable under CPA.	TBD. Under EDPB guidelines, review DPIA to determine if processing is performed in accordance with the DPIA, at least when there is a change of the risk, and update the DPIA periodically. See also CPA regarding annual DPIA for profiling.	California law will likely require making DPIAs available to the California Attorney General upon request and may potentially require filing with the CPPA in some or all circumstances.
ICDPA	Required for processing activities created or generated on or after January 1, 2026, and when: - Processing for targeted advertising, - Selling personal data - Processing for profiling that presents certain risks, - Processing sensitive data, - Other processing activities involving a heightened risk of harm to consumers.	Identify and weigh the benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against potential risks to the rights of the consumer associated with such processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of consumers, the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed.	N/A	N/A	Controllers must disclose a DPIA to the Indiana AG upon request. The DPIA will remain confidential and exempt from disclosure.

	Timing	Content	Storage	Updates	Government Access
TIPA	Required for processing activities created or generated on or after July 1, 2024, and when: - Processing for targeted advertising, - Selling personal data - Processing for profiling that presents certain risks, - Processing sensitive data, - Other processing activities involving a heightened risk of harm to consumers.	Identify and weigh the benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against potential risks to the rights of the consumer associated with such processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of consumers, the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed.	N/A	N/A	Controllers must disclose a DPIA to the Tennessee AG and reporter upon request. The DPIA will remain confidential and exempt from disclosure.
CAADCA	Required before any new online services, products, or features likely to be accessed by children is offered to the public. The law goes into effect for services offered to the public on or after July 1, 2024.	Identify the purpose of the online service, product or feature ("online service"), how it uses children's personal information, the risks of material detriment to children that arise from the data management practices of the company, and a timed plan to mitigate risks. DPIAs must address if the service's: (1) design could harm children; (2) design could lead to children experiencing harmful, or potentially harmful, contacts; (3) design could permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct; (4) design could allow children to be party to or exploited by a harmful, or potentially harmful, contact; (5) algorithms could harm children; (6) Targeted advertising systems could harm children; (7) design features could increase, sustain, or extend use of the service by children; and (8) practices include collection or processing sensitive data of children.	Maintain the DPIA for as long as the online service is likely to be accessed by children.	Biennially review DPIA.	Company must provide a list of all DPIAs completed within three business days of a written request by the California AG. Company must also make a DPIA available to the AG within five business days of a written request. The DPIA will be confidential and exempt from disclosure.
MCDPA	Required for processing activities created or generated after January 1, 2025, that present a heightened risk of harm to consumers, including: - Processing for targeted advertising, - Selling personal data - Processing for profiling that presents certain risks, - Processing sensitive data.	Identify and weigh the benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against potential risks to the rights of the consumer associated with such processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of consumers, the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed.	N/A	N/A	Controllers must disclose a DPIA to the Montana AG upon request. The DPIA will remain confidential and exempt from disclosure.

	Timing	Content	Storage	Updates	Government Access
FLORIDA LAW*	Required for processing activities generated on or after July 1, 2023, and when: - Processing for targeted advertising, - Selling personal data - Processing for profiling that presents certain risks, - Processing sensitive data. - Other processing activities involving a heightened risk of harm to consumers.	Identify and weigh the benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against potential risks to the rights of the consumer associated with such processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of consumers, the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed.	N/A	N/A	Controllers must disclose a DPIA to the Florida AG upon request. The disclosure of the DPIA to the Florida AG will not constitute a waiver of attorney-client privilege or work product protection.