SQUIRE PATTON BOGGS

Data Protection Assessment Requirements: Comparative Chart

	VCDPA	CPA	CTPA	CPRA	CAADCA
Timing	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, - For other processing activities involving a heightened risk of harm to Consumers.	Required for Processing activities conducted or generated after July 1, 2023, and before initiating certain activities, including: - Sale of Personal Data, - Processing of Sensitive Data, - Processing for Targeted Advertising, - Processing for Profiling that presents certain risks, - other substantial injury to Consumers.	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, - For other processing activities involving a heightened risk of harm to Consumers.	TBD, but potentially everything required by CPA plus regarding "sharing" and the following that come from the European Data Protection Board (EDPB) Guidelines the CPPA has stated that they are looking to in addition to the CPA regulations: Required prior to processing that is likely to result in a high risk to the rights and freedoms of natural persons, 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.	Required before any new online services, products, or features likely to be accessed by children are offered to the public. The law goes into effect for services offered to the public on or after July 1, 2024.

Content	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.	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 Regulations also require 12 specific pieces of information, including an additional 12 if profiling.	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.	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 regulations: At a minimum, assessments 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.	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. Assessments must address if the service's: - design could harm children; - design could lead to children experiencing harmful, or potentially harmful, contacts; - design could permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct; - design could allow children to be party to or exploited by a harmful, or potentially harmful, contact; - algorithms could harm children; - Targeted Advertising systems could harm children; - design features could increase, sustain, or extend use of the service by children; and - practices include the collection or processing of Sensitive Personal Data of children.

Storage	N/A	Data protection assessments must be stored for as long as the Processing activity continues, and for at least three (3) years after it has concluded.	N/A	TBD. N/A under EDPB, but applicable under CPA.	Maintain the assessment for as long as the service is likely to be accessed by children.
Updates	N/A	Review and update the assessment as often as appropriate considering type, amount, sensitivity of data, and level of risk. If Profiling, review and update the assessment at least annually.	N/A	TBD. Under EDPB guidelines, review assessment to determine if Processing is performed in accordance with the data protection assessment, at least when there is a change of the risk, and update the data protection assessment periodically. See also CPA regarding annual assessment for profiling.	Biennially review assessment.
Government Access	Controllers must disclose a data protection assessment to the Virginia AG upon request. Data protection assessments will be confidential and exempt from disclosure.	Controllers must disclose a data protection assessment to the Colorado AG within 30 days of the AG's request. The data protection assessment will be confidential and exempt from disclosure.	Controllers must disclose a data protection assessment to the Connecticut AG upon request. The data protection assessment will remain confidential and exempt from disclosure.	California law will likely require making data protection assessments available to the California Attorney General upon request and may potentially require filing with the CPPA in some or all circumstances.	Company must provide a list of all data protection impact assessments completed within three business days of a written request by the California AG. Company must also make a data protection impact assessment available to the AG within five business days of a written request. The data protection assessment will be confidential and exempt from disclosure.