DI&A Requirements: Comparative Chart

Law	Timing	Content	Storage	Updates	Government Access
California (CCPA)	TBD, but potentially everything required by CPA plus regarding "Sharing" of Personal Data, and the following, which come from a discussion draft of potential California regulations: Required prior to Processing that presents significant risk to data subjects' privacy, including for the following activities: - ***Selling or Sharing Personal Data*** - ***Processing Sensitive Personal Data, other than that of employees or independent contractors for employment purposes;*** - ***Using Automated Decisionmaking Technology for (1) a decision that produces legal or significant effect, (2) Profiling employees, independent contractors, job applicants, or students, (3) Profiling data subjects in a publicly accessible place, and (4) Profiling for Behavioral Advertising;*** - ***Processing Personal Data of data subjects the business has actual knowledge are under age 16;*** - ***Processing of Personal Data to train Automated Decisionmaking Technology or Artificial Intelligence.*** Currently proposed to cover practices crated or generated after the effective date of the regulations, but to provide two years from that date to complete the assessments and file summaries.	TBD, but potentially everything required by CPA and the following, which come from the CA Discussion Regs: At a minimum, assessments must contain the following information: - ***A short summary of the Processing activity*** - ***Categories of Personal Data processed*** - ***Context of the Processing activity*** - ***data subjects' reasonable expectations concerning the purpose for Processing*** - ***Operational elements of Processing*** - ***Purposes of the Processing*** - ***Benefits and negative impacts associated with Processing*** - ***Safeguards to address the negative impacts*** - ***Risk/ benefit analysis*** - ***Relevant internal actors and external parties that have contributed to the DI&A*** - ***Any external or internal audits conducted*** - ***Dates the DI&A was reviewed and approved, and presented to the business's highest ranking executive*** - ***Names, positions, and signatures of individuals responsible for review and approval***	TBD. Under the CA Discussion Regs, DI&As must be retained for as long as the Processing continues, and for at least 5 years after competition of the DI&A or Processing.	TBD. Under CA Discussion Regs, review and update the DI&A whenever there is a material change, or at least once every three years, potentially more frequently for use of Automated Decisionmaking Technology.	California law will likely require filing summaries of assessments with the CPPA annually. Full assessments are to be available to the CPPA or California Attorney General upon request.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is limited to ANA members. Consult legal counsel with regard to use of the materials. Copyright 2024, Squire Patton Boggs (Ireland). Current as of October 4, 2024.

Law	Timing	Content	Storage	Updates	Government Access
California Age Appropriate Design Act (CAADCA)	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, but is currently being challenged under first amendment grounds. The assessment requirements have been struck as unconstitutional. See Netchoice, LLC v Rob Bonta, Atty General of the State of California (9th Cir., August 16, 2024) – a copy of the opinion is here. The appeals court, however, overruled the district court as to the injunction of other provisions of CAADCA, such as restrictions on the collection, use, and sale of minor's personal data and how data practices are communicated. See above regarding similar recent amendments to Connecticut's privacy law.	Identify the purpose of the online service, product, or feature (online service), how it uses Children's Personal Data, 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*** Practices include Collection or Processing Sensitive Data of Children	Maintain the DI&A for as long as the online service is Likely to be Accessed by Children.	Biennially review the DI&A.	The company must provide a list of all assessments completed within three business days of a written request by the California attorney general. The company must also make a DI&A available to the attorney general within five business days of a written request. The DI&A will be confidential and exempt from disclosure.
Colorado (CPA)	Required for Processing activities conducted or generated after July 1, 2023, and before initiating certain activities, including: - ***Selling Personal Data*** - ***Processing Sensitive Data*** - ***Processing for Targeted Advertising*** - ***Processing for Profiling that presents certain risks*** - ***Other Processing activities involving a heightened risk of harm to data subjects***	Identify and describe the risks to the rights of data subjects 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 (CPA Regs) also require 12 specific pieces of information, including an additional 12 if Profiling.	Assessments must be stored for as long as the Processing activity continues, and for at least three years after it has concluded.	Review and update the DI&A as often as appropriate, considering type, amount, sensitivity of data, and level of risk. If Profiling, review and update the DI&A at least annually.	Controllers must disclose a DI&A to the Colorado attorney general within 30 days of the attorney general's request. The DI&A will be confidential and exempt from disclosure.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is limited to ANA members. Consult legal counsel with regard to use of the materials. Copyright 2024, Squire Patton Boggs (Ireland). Current as of October 4, 2024.

Law	Timing	Content	Storage	Updates	Government Access
Colorado AI Act (CO-AI Act)	On or after February 1, 2026, a deployer, or a third party contracted by the deployer, that deploys a high-risk AI system must complete a DI&A.	There are eight specific inquiries that need to be addressed, including a description of the purpose and intended use cases, categories of Personal Data processed as inputs, details about customization of the high-risk AI system, metrics to evaluate performance and limitations, and a description of transparency and monitoring measures taken.	Maintain all records concerning DI&As for at least three years following the final deployment of the high-risk AI.	DI&A must be completed at least annually, and within 90 days after any intentional and substantial modification to the high-risk AI.	Deployers must make a DI&A available to the Colorado Attorney General upon request. The DI&A will not be subject to disclosure under the Colorado Open Records Act, and its disclosure will not constitute a waiver of attorney-client privilege or work product protection.
Connecticut (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 (including Consumer Health Data [see WA MHMD/Nevada Consumer Health Data Law]*** - ***Services reasonably accessible by Minors [see CA AADA]*** - ***Other Processing activities involving a heightened risk of harm to data subjects***	Identify and weigh the benefits that may flow, directly and indirectly, from the Processing to the Controller, the data subject, other stakeholders, and the public, against potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must disclose a DI&A to the Connecticut attorney general upon request. The DI&A will remain confidential and exempt from disclosure.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is limited to ANA members. Consult legal counsel with regard to use of the materials. Copyright 2024, Squire Patton Boggs (Ireland). Current as of October 4, 2024.

Law	Timing	Content	Storage	Updates	Government Access
Delaware (DPDPA)	Required for Controllers who process the personal data of at least 100,000 consumers and for Processing activities created or generated on or after July 1, 2025, that present a heightened risk of harm to data subjects, including: - ***Processing for Targeted Advertising*** - ***Selling Personal Data*** - ***Processing for Profiling that presents certain risks*** Processing Sensitive Data	Identify and weigh how the Processing may directly or indirectly benefit the Controller, the data subject, other stakeholders, and the public against the potential risks to the data subject associated with that Processing as mitigated by safeguards. Factor in the use of deidentified data, the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subjects whose Personal Data will be processed.	N/A	N/A	Controllers must make DI&As available to the Delaware attorney general upon request, if the DI&A is relevant to an investigation the attorney general conducts. The DI&A will remain confidential and exempt from public inspection and copying, and its disclosure will not constitute a waiver of attorney-client privilege or work product protection.
Florida (FL-DBR)	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 data subjects	Identify and weigh the benefits that may flow, directly or indirectly, from the Processing to the Controller, the data subject, other stakeholders, and the public against potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must disclose a DI&A to the Florida attorney general upon request. The disclosure of the DI&A to the Florida attorney general will not constitute a waiver of attorney-client privilege or work product protection.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is limited to ANA members. Consult legal counsel with regard to use of the materials. Copyright 2024, Squire Patton Boggs (Ireland). Current as of October 4, 2024.

Law	Timing	Content	Storage	Updates	Government Access
Indiana (ICDPA)	Required for Processing activities created or generated after December 31, 2025, 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 data subjects	Identify and weigh the benefits that may flow, directly and indirectly, from the Processing to the Controller, the data subject, other stakeholders, and the public, against potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must disclose a DI&A to the Indiana attorney general upon request. The DI&A will remain confidential and exempt from disclosure.
Kentucky (KY-CDPA)	Required for Processing activities created or generated on or after June 1, 2026, including: - ***Processing for Targeted Advertising*** - ***Selling Personal Data*** - ***Processing for Profiling that presents certain risks*** - ***Processing Sensitive Data*** - ***Other Processing that presents a heightened risk of harm to data subjects.***	Identify and weigh the benefits that may flow, directly and indirectly, from the Processing to the Controller, the data subject, other stakeholders, and the public against potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must make DI&As available to the Kentucky Attorney General upon request. The DI&A will remain confidential and exempt from public inspection, and its disclosure will not constitute a waiver of any attorney-client privilege or work product protection.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is limited to ANA members. Consult legal counsel with regard to use of the materials. Copyright 2024, Squire Patton Boggs (Ireland). Current as of October 4, 2024.

Law	Timing	Content	Storage	Updates	Government Access
Maryland (MODPA)	Required for Processing activities that occur on or after October 1, 2025, that present a heightened risk of harm to a data subject, including an assessment for each algorithm used and: - ***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, directly and indirectly, from the Processing to the Controller, the data subject, other interested parties, and the public against potential risks to the rights of the data subject associated with the Processing as mitigated by safeguards. Also factor in the necessity and proportionality of Processing in relation to the stated purpose of the Processing, the use of deidentified data, the reasonable expectations of data subjects, the context of Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must make DI&As available to the Maryland Division of Consumer Protection in the Attorney General's office upon request. The DI&A will remain confidential and exempt from public inspection, and its disclosure shall not constitute a waiver of any attorney-client privilege or work product protection.
Minnesota (MN-CDPA)	As of July 31, 2025, required for each of the following Processing activities: - ***Processing for Targeted Advertising*** - ***Selling Personal Data*** - ***Processing for Profiling that presents certain risks*** - ***Processing Sensitive Data*** - ***Other Processing that presents a heightened risk of harm to data subjects.***	Take into account the type of Personal Data to be processed by the Controller, including the extent to which the Personal Data is Sensitive Data and the context in which the Personal Data is to be processed. Identify and weigh the benefits that may flow, directly and indirectly, from the Processing to the Controller, the data subject, other stakeholders, and the public against the potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of deidentified data and the reasonable expectations of data subjects, as well as the context of the Processing and the relationship between the Controller and the data subject whose Personal Data will be processed. DI&As must also include a description of Controller's policies and procedures that Controller has adopted to comply with the law.	N/A	N/A	Controllers must make DI&As available to the Minnesota Attorney General upon request. The DI&A will be classified as nonpublic data, and its disclosure will not constitute a waiver of attorney-client privilege or work product protection.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is limited to ANA members. Consult legal counsel with regard to use of the materials. Copyright 2024, Squire Patton Boggs (Ireland). Current as of October 4, 2024.

Law	Timing	Content	Storage	Updates	Government Access
Montana (MCDPA)	Required for Processing activities created or generated after January 1, 2025, that present a heightened risk of harm to data subjects, 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, directly and indirectly, from the Processing to the Controller, the data subject, other stakeholders, and the public against potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must disclose a DI&A to the Montana attorney general upon request. The DI&A will remain confidential and exempt from disclosure.
Nebraska (NDPA)	As of January 1, 2025, required for the following Processing activities: - ***Processing for Targeted Advertising*** - ***Selling Personal Data*** - ***Processing for Profiling that presents certain risks*** - ***Processing Sensitive Data*** Other Processing that presents a heightened risk of harm to data subjects	Identify and weigh the benefits that may flow, directly and indirectly, from the Processing to the Controller, the data subject, other stakeholders, and the public against potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must make DI&As available to the Nebraska Attorney General upon request. The DI&A will remain confidential and exempt from public inspection, and its disclosure will not constitute a waiver of any attorney-client privilege or work product protection.
New Hampshire (NH-CDPA)	Required for Processing activities created or generated after July 1, 2024, that present a heightened risk of harm to data subjects, 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, directly or indirectly, from the Processing to the Controller, the data subject, other stakeholders, and the public against potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must make DI&As available to the New Hampshire Attorney General upon request. The DI&A will remain confidential and exempt from public inspection, and its disclosure shall not constitute a waiver of any attorney-client privilege or work product protection.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is limited to ANA members. Consult legal counsel with regard to use of the materials. Copyright 2024, Squire Patton Boggs (Ireland). Current as of October 4, 2024.

Law	Timing	Content	Storage	Updates	Government Access
New Jersey (NJ_CDPA)	Required for Processing activities that involve Personal Data acquired on or after January 16, 2025, that present a heightened risk of harm to data subjects, 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, directly and indirectly, from the Processing to the Controller, the data subject, other stakeholders, and the public against potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must make DI&As available to the Division of Consumer Affairs in the Department of Law and Public Safety upon request. The DI&A will remain confidential and exempt from public inspection, and its disclosure shall not constitute a waiver of any attorney-client privilege or work product protection.
Oregon (OR-CDPA	Required for Processing activities that occur on or after July 1, 2024, that present a heightened risk of harm to data subjects, including: - ***Processing for Targeted Advertising*** - ***Selling Personal Data*** - ***Processing for Profiling that presents certain risks*** Processing Sensitive Data	Identify and weigh how the Processing may directly or indirectly benefit the Controller, the data subject, other stakeholders, and the public against the potential risks to the data subject associated with that Processing as mitigated by safeguards. Factor in the use of deidentified data, the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subjects whose Personal Data will be processed.	A Controller must retain DI&As for at least five years.	N/A	Controllers must make DI&As available to the Oregon attorney general upon request, if the DI&A is relevant to an investigation the attorney general conducts. The DI&A will remain confidential and exempt from public inspection and copying, and its disclosure will not constitute a waiver of attorney-client privilege or work product protection.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is limited to ANA members. Consult legal counsel with regard to use of the materials. Copyright 2024, Squire Patton Boggs (Ireland). Current as of October 4, 2024.

Law	Timing	Content	Storage	Updates	Government Access
Rhode Island (RI-DTPPA)	As of January 1, 2026, required for each of the following Processing activities created or generated after such date: - ***Processing for Targeted Advertising*** - ***Selling Personal Data*** - ***Processing for Profiling that presents certain risks*** - ***Processing Sensitive Data*** - ***Other Processing that presents a heightened risk of harm to data subjects.***	No specific requirements.	N/A	N/A	Controllers must make DI&As available to the Rhode Island Attorney General upon request. The DI&A will be classified as nonpublic data, and its disclosure will not constitute a waiver of attorney-client privilege or work product protection.
Tennessee (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 data subjects***	Identify and weigh the benefits that may flow, directly and indirectly, from the Processing to the Controller, the data subject, other stakeholders, and the public, against potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must disclose a DI&A to the Tennessee attorney general and reporter upon request. The DI&A will remain confidential and exempt from disclosure.
Texas (TDPSA)	Required for Processing activities generated after January 1, 2025, including: - ***Processing for Targeted Advertising*** - ***Selling Personal Data*** - ***Processing for Profiling that presents certain risks*** - ***Processing Sensitive Data*** - ***Other Processing that presents a heightened risk of harm to data subjects.***	Identify and weigh the direct or indirect benefits that may flow from the Processing to the Controller, the data subject, other stakeholders, and the public against the potential risks to the rights of the data subject associated with that Processing as mitigated by safeguards. Factor in the use of deidentified data, the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must make DI&As available to the Texas attorney general pursuant to a civil investigative demand. The DI&A will remain confidential and exempt from public inspection and copying, and its disclosure will not constitute a waiver of attorney-client privilege or work product protection.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is limited to ANA members. Consult legal counsel with regard to use of the materials. Copyright 2024, Squire Patton Boggs (Ireland). Current as of October 4, 2024.

Law	Timing	Content	Storage	Updates	Government Access
Virginia (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 data subjects	Identify and weigh the benefits that may flow, directly and indirectly from the Processing to the Controller, the data subject, other stakeholders, and the public, against potential risks to the rights of the data subject associated with such Processing as mitigated by safeguards. Factor in the use of de-identified data and the reasonable expectations of data subjects, the context of the Processing, and the relationship between the Controller and the data subject whose Personal Data will be processed.	N/A	N/A	Controllers must disclose a DI&A to the Virginia attorney general upon request. The DI&A will be confidential and exempt from disclosure.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is limited to ANA members. Consult legal counsel with regard to use of the materials. Copyright 2024, Squire Patton Boggs (Ireland). Current as of October 4, 2024.

POWERED BY SPB: (1) This is not legal advice, it's educational reference material and (2) There's no attorney-client relationship with Squire Patton Boggs (SPB) unless a written attorney-client engagement agreement is entered into with SPB. Use of these materials is subject to the terms of the license between the end user and SPB, including limiting access and use to the licensee. Consult legal counsel with regard to use of the materials.