SQUIRE PATTON BOGGS

exterro ankura

Data Risk Assessments - Artificial Intelligence and Privacy Impact Assessments

A Review of the Latest U.S. State Regulatory Requirements and Scalable Implementation Strategies

November 11, 2024 -- 1:45 pm

Panel Introductions

Squire Patton Boggs

Alan Friel

Partner

alan.friel@squirepb.com

+213.624.2500

- Chair of SPB's Data Privacy, Cybersecurity and Digital Assets Practice
- Los Angeles
- CIPP/CIPM

Ankura Consulting

David Manek

Senior Managing Director, Cybersecurity & Data Privacy

david.manek@ankura.com

+773.368.3461

- Global Data Privacy and AI Regulatory Compliance Practice Leader
- Chicago

Exterro, Inc.

Taylor Ball, CIPM

Account Manager - West

taylor.ball@exterro.com

Kellanova

Kimberly Wong

Vice President, Chief Counsel

kimberly.wong@kellanova.com

Agenda

1. **The purposes for and history of data practices assessments**
2. **U.S. state privacy laws' requirements for assessments.**
3. **A.I. Impact Assessment** – How to extend privacy impact assessments to include questions to support ethical A.I. governance.
4. **Operationalizing Privacy and AI Impact Assessments** – How to operationalize a privacy and AI impact assessment process using a pre-developed toolkits and privacy management technology.
5. **Constitutional Questions**
6. **Take aways and Q&A**

SQUIRE PATTON BOGGS

ankura

exterro

Assessments

Background

Privacy Impact Assessments

- Identify and mitigate risk
- Keep RoPAs / data inventories evergreen
- Part of Privacy-by-Design
  - Including data minimization
- Increasingly required for:
  - High risk personal data processing
  - Potential harms of consequential decisions from ADM/Profiling
  - Algorithmic Bias
  - To meet program standards

Applying the High Water Mark

Assessment Required

- Processing **Sensitive Data**
- Processing Personal Data for **Targeted Advertising**
- **Selling** Personal Data
- Processing Personal Data for **high-risk Processing**
- **Profiling that has a significant impact** on the data subject
- **Using automated decision-making technology for** (1) a decision that produces **legal or similarly significant effects** concerning a Consumer, (2) **Profiling a** Consumer acting in their capacity **as an employee, job applicant, independent contractor, or student**, (3) **Profiling a Consumer in a publicly accessible place**, or (4) Profiling for **Behavioral Advertising** (CA Discussion Draft Regs).
- Processing the Personal Data of **Children/ Minors** (U.S. Privacy Laws (included under Sensitive Data), and CA Discussion Draft Regs and CA Age Appropriate Design Act).

Other (EDPB and CA Draft Regs)

- Systemic and extensive evaluations based on automated Processing (EDPB and CA)
- Processing data on a large scale (EPDB)
- Processing the Personal Data of data subjects to train AI or ADM technology (CA Discussion Draft Regs).
- Matching or combining data sets in a way that would exceed the reasonable expectations of a Consumer (EDPB guidelines)(related to purpose limitation requirements under U.S. State Privacy Laws).
- Innovative use or use of new technology (EDPB)
- Processing itself prevents data subjects from exercising a right or using a service (EDPB guidelines) (CA Discussion Draft Regs as to ADM)
- Use of cookies or other tracking technologies
- When a security incident would trigger an obligation to notify data subjects or the government (not explicitly required but recommended).

Assessment Contents

Assessments should document:

- Summary of the Processing activity;
- Personal Data involved in the Processing activity;
- Context and purposes of Processing;
- Risk-benefit analysis of the Processing activity;
  - Identification of potential risks and harms and description of measures taken to address risks;
  - Identification of the potential benefits of the Processing activity;
- Identification of internal and external actors involved in the Processing activity, including all data recipients; and
- Other specific requirements enumerated in the applicable laws.

SQUIRE PATTON BOGGS

ankura

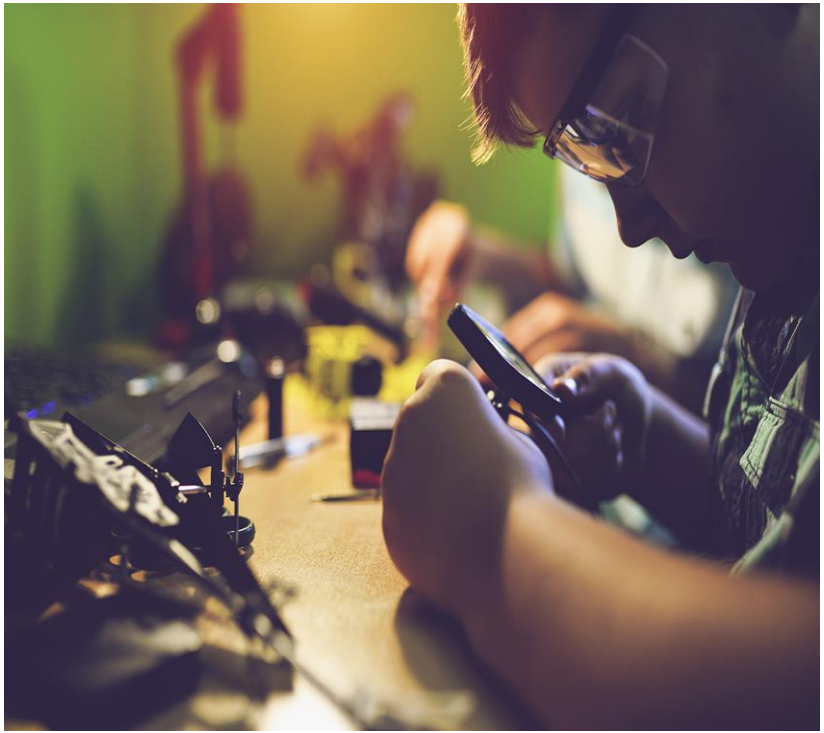
exterro

Colorado

Privacy Act & AI Law

Colorado's Privacy Act

- There are 12 primary things an assessment must consider and document
- If concerning profiling, there are 12 additional requirements to assess foreseeable risk of harm
- 11 potential risks of harm should also be considered
- The ability to comply with CPA obligations and consumer rights
- Maintain for inspection
- Regular updates



CO AI Act

As of January 1, 2026

- If it is not ultimately prompted by federal law, will require compliance obligations apply to a High-Risk Artificial Intelligence System ("*HAIS*").

- A HAIS is an "Artificial Intelligence System" that when deployed makes or is a "Substantial Factor" in making a "Consequential Decision."

- There are **duties of care** for "Developers," and "Deployers" to protect against "Algorithmic Discrimination" or other harms with specific responsibilities, including that:
  - Deployers conduct assessments
  - Developers have provide information to enable such assessments

Deployers Must Assess and Manage Risks

Using NIST or equivalent frameworks

- **Risk Management Policy and Program:** Implement a risk management policy and program for HAIS use that includes specific "principles, processes and personnel," including use of risk assessments, to identify, document and mitigate known or reasonably foreseeable risks of Algorithmic Discrimination and other harms over the HAIS' lifecycle.

- **Impact Assessment**: Complete an impact assessment for deployed HAIS at least annually and within 90 days after any intentional and substantial modification to the HAIS (Colo. Rev. Stat. § 6-1-1703(3).) The impact assessment must meet specific content requirements including: **a description of inputs and outputs; metrics used to evaluate performance and limitations; a description of transparency measures; and a plan for post-deployment monitoring.**

SQUIRE PATTON BOGGS

ankura

exterro

California

CPPA Draft Regulations on Assessments

Additional requirements beyond Colorado

- A combination of Colorado and EDPB, with some unique requirements on top of that.
- More on AI training and ADM and Profiling, including “behavioral advertising”
- Must include all internal and external parties contributing to the data practice and documents their involvement in the assessment
- Certification by approvers
- Copies of external and external audits and supporting information
- Filing of abridged versions

More Detail on Operational Elements

- Planned method for Processing and retaining Personal Data,
- Sources of Personal Data Collected,
- How Company complies with data minimization requirements,
- Retention period for each category of Personal Data, including criteria to determine that period,
- Relationship between the data subject and Company,
- Approximate number of data subjects whose Personal Data the Company plans to process,
- Disclosures Company has made or plans to make about the Processing, how those disclosures are made, and how Company ensures they are specific, explicit, prominent, and clear to the data subject,
- Technology used in the Processing,
- Names of Service Providers, Contractors, or Third Parties to whom Personal Data is disclosed, including purposes for disclosures, and how Company ensures that data subjects are aware of the involvement of these entities in the Processing,
- Outputs of the ADM or AI System, and
- An explanation of the logic of the ADM or AI System, if used.

Failed Constitutional challenge:

- Would have required a DPIA:
  - Identify the purpose of the online service, product, or feature,
  - Describe how it uses Minors' Personal Data, and
  - Discuss the risks of material detriment to Minors that arise from the data management practices.
- The DI&A would have required responding to 8 specific questions to gauge potential harm.

SQUIRE PATTON BOGGS

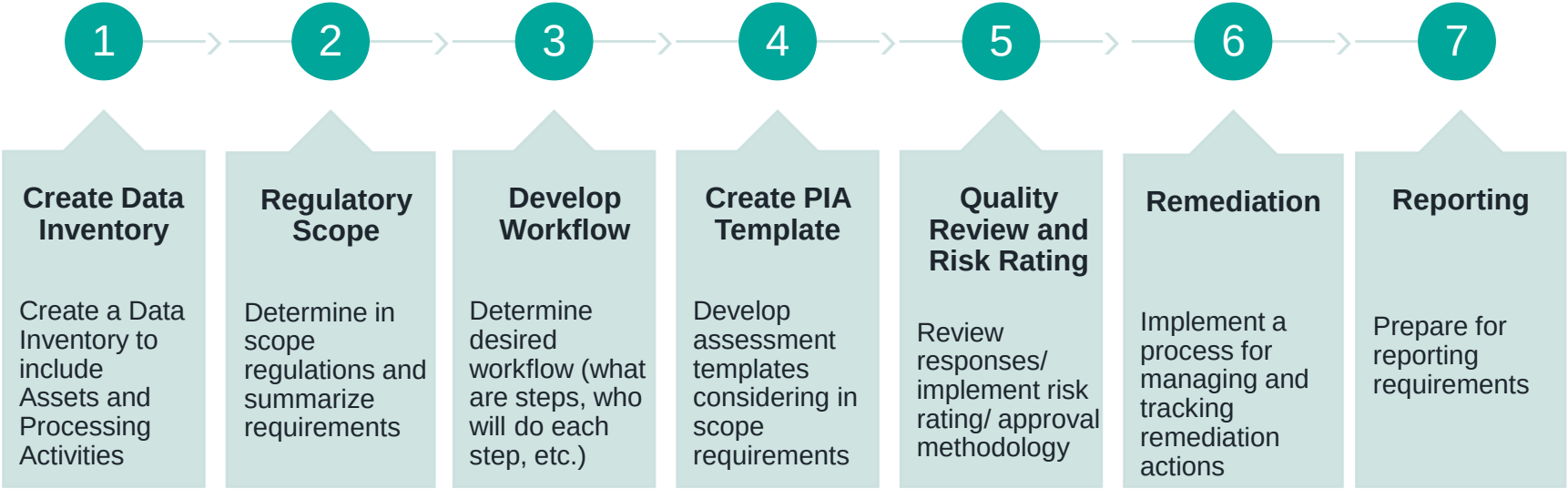
ankura

exterro

Operationalizing Privacy and AI Impact Assessments

Steps to Operationalize Privacy and AI Impact Assessments

exterro ankura SQUIRE PATTON BOGGS



Step 1: Create Data Inventory

exterro ankura SQUIRE PATTON BOGGS

Data Asset Assessments

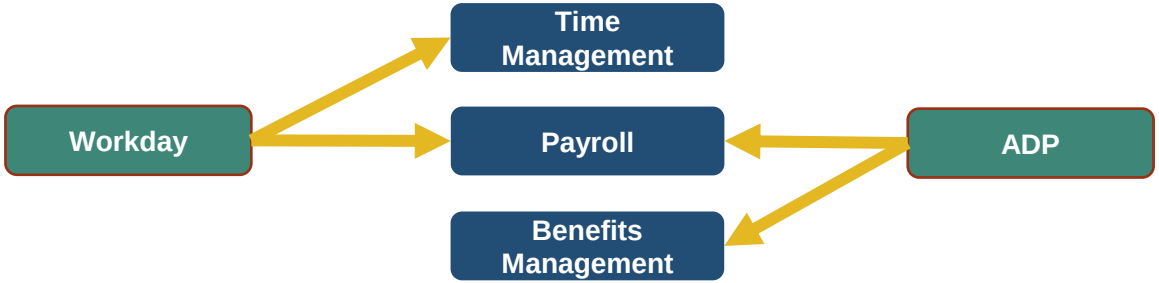
- An **data asset** refers to a “place” (typically an electronic system) that stores or processes personal information or critical/proprietary information. (e.g., application, website, database)
- *Ex. Systems like Salesforce, Workday, etc.*

Data Inventory

Processing Activity Assessments

- A **processing activity** refers to any process or operation which collects, stores (in an asset), manipulates and potentially transfers personal information or critical/proprietary information
- *Ex. Direct Marketing, Recruiting, Processing Payment, etc.*

Assets and processing activities can have many-to-many relationships



Step 2: Determine Regulatory Requirements in Scope

exterro ankura SQUIRE PATTON BOGGS

EXHIBIT A

DI&A Requirements: Comparative Chart

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.
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.

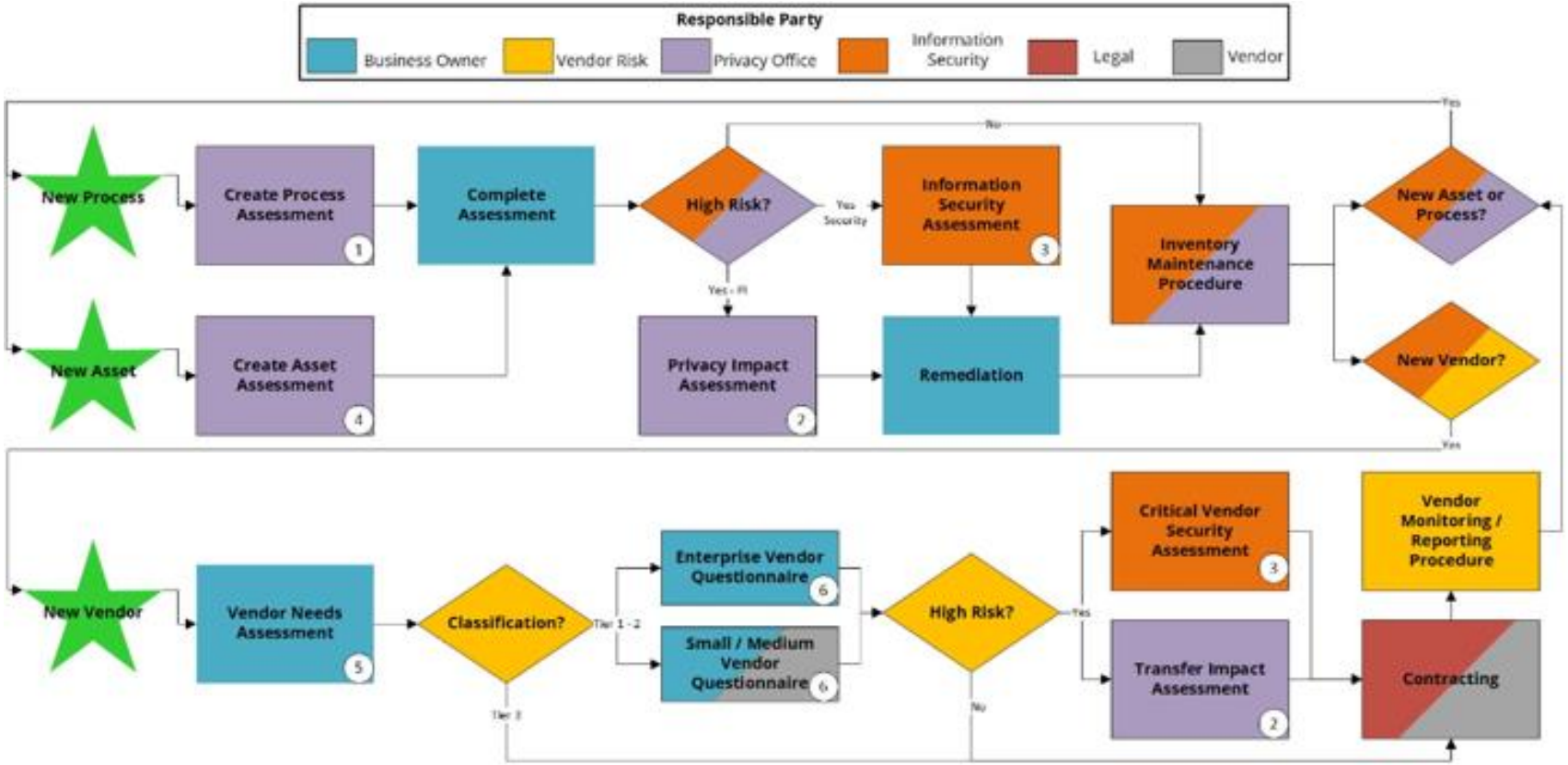
Both Ankura and Exterro have developed SPB Powered Data Inventory and Assessment Toolkits Which Include Comparative Charts and Templates.

Step 2: Determine Regulatory Requirements in Scope

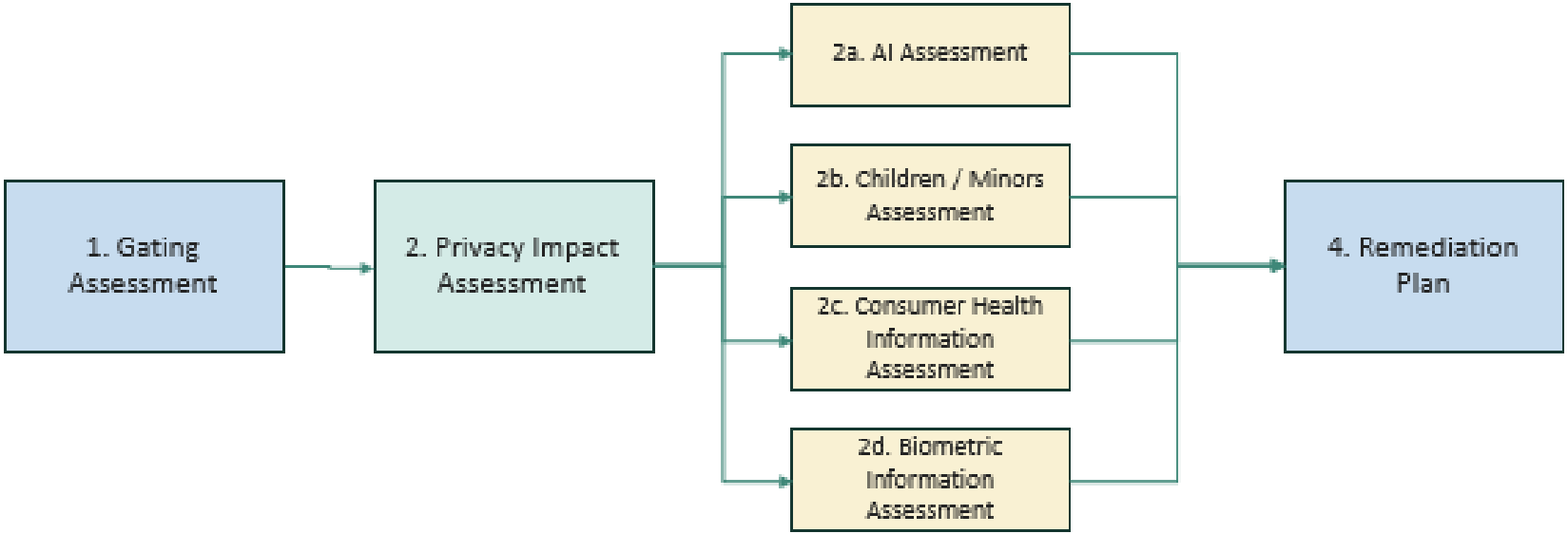
Consider Separate Questions or Assessment to Assess AI Activities (examples below):

1. Describe all intended uses of the system/ process.
    a) Describe who will use it.
    b) Describe what it will be used to accomplish.
    c) Describe where it will be used.
    d) Describe why automated Processing is preferred to manual Processing.
2. Indicate whether there will be human involvement in the AI or ADM/Profiling process, including any appeals process. If yes:
    a) Describe the human involvement, including its role and purpose(s).
    b) If Company will not act on an opt-out request because of human-involvement (CO only), describe the process for notifying Colorado data subjects.
3. Indicate whether Personal Data will serve as input data or training data for the AI or ADM/Profiling system
4. Indicate whether there is a risk of algorithmic bias with the use of the AI or ADM/Profiling system for the Processing activity.
5. Indicate whether Company uses bots to communicate or interact with Consumers.

Step 3: Determine Desired Workflow



Step 3: Determine Desired Workflow



Step 4: Develop PIA Template

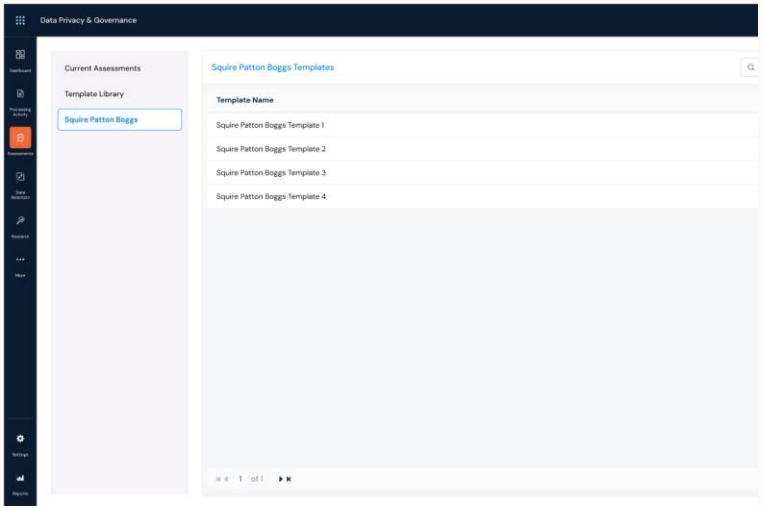
Benefits Include:

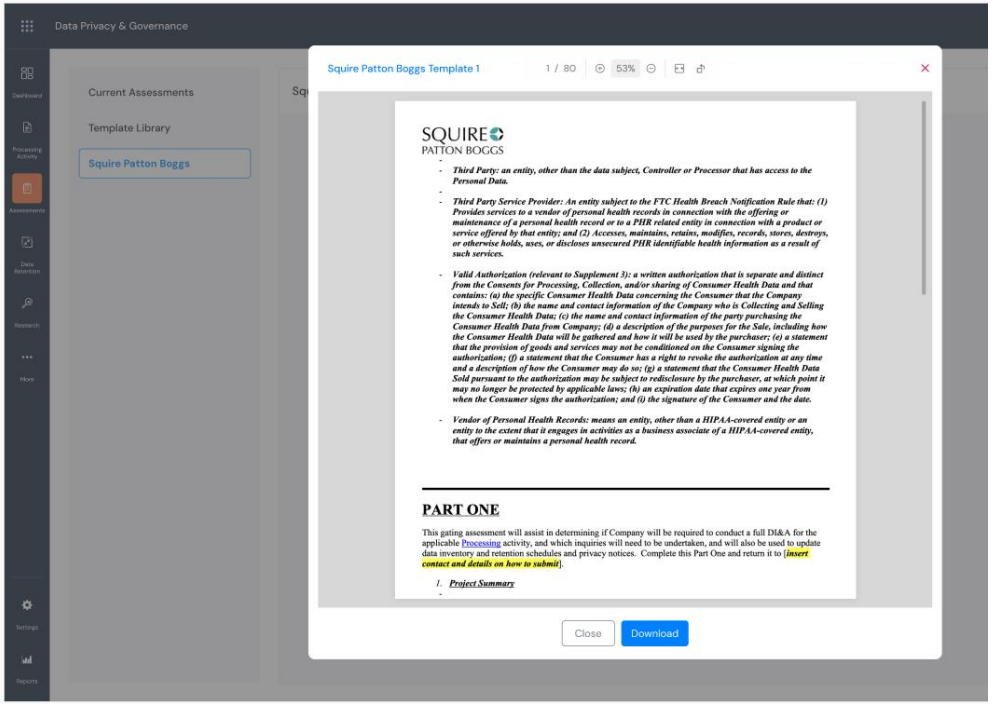
1. Customized, user-friendly assessments.
2. Use of conditional logic which shows or hides questions, sections, or content based on how respondents answer previous questions.
3. Customized rules to auto launch additional assessments based on respondents' answers.
4. Collaboration between business owners and IT owners.
5. The ability to make questions required.
6. The ability to capture details on Data Subjects, Categories and Elements.
7. Seamless integration between the PIA process, Data Inventory, Data Mapping, and Third-Party Risk Management.
8. A record of findings, risk, controls and remediation actions.
9. Customized workflows that allow automation of notifications and tasks.
10. A log of all changes and versioning control.
11. Customized reports and dashboards.

Step 4: Examples of Assessments

Leverage SPB templates in Exterro

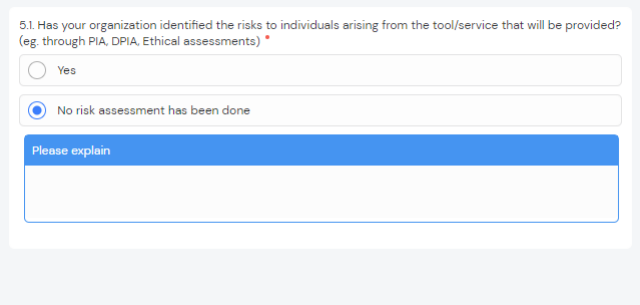
Announcing Exterro's new template library!



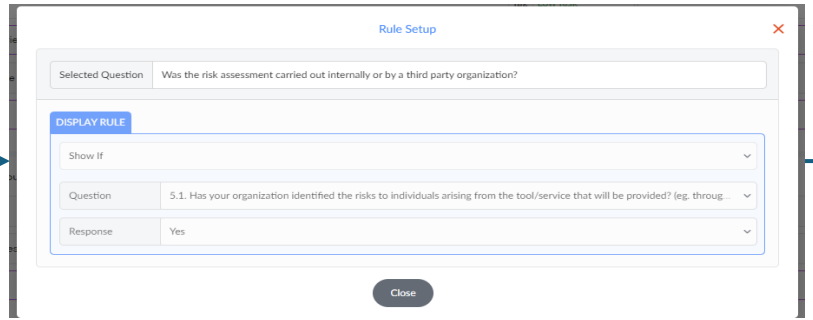


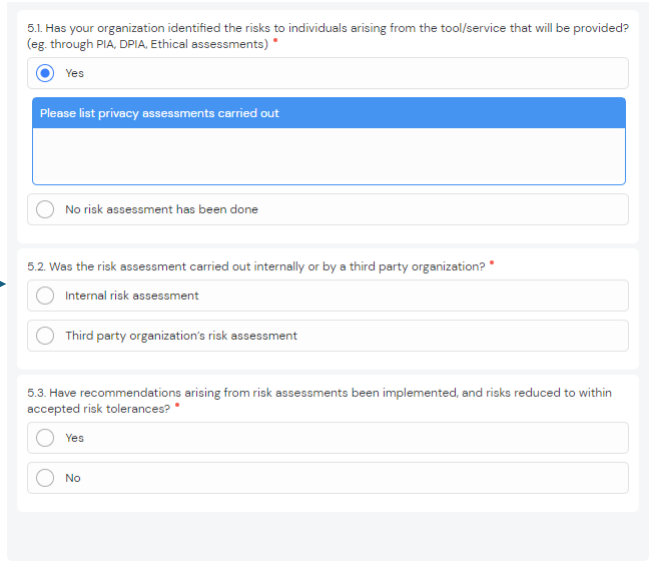
Step 4: Examples of Assessments

Conditional Logic Example: If user answer “Yes” to question 5.1 below:



..that prompts additional follow-up questions which appears below question 5.1

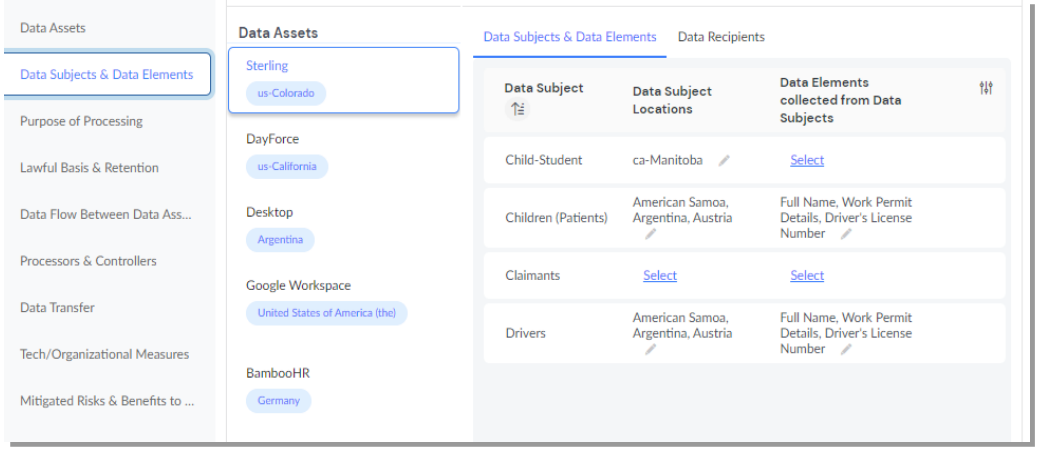


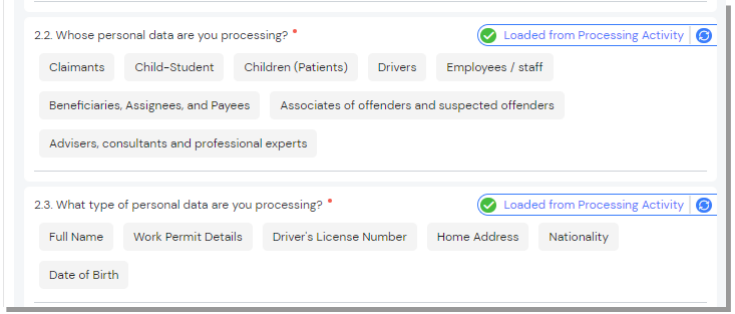


Examples of Assessments

Full integration between Assessment Manager and RoPA Manager

Information captured in a Processing Activity is automatically synchronized with a DPIA, so that it removes discrepancies and reduces time – no need to answer redundant questions.



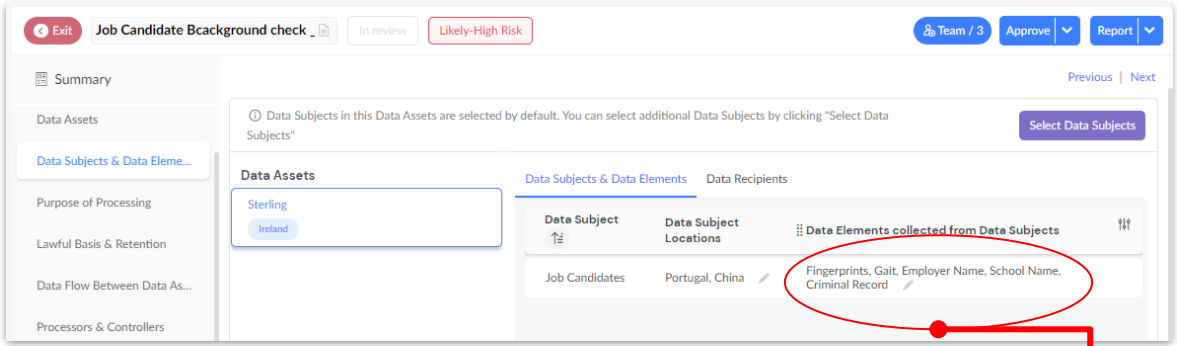


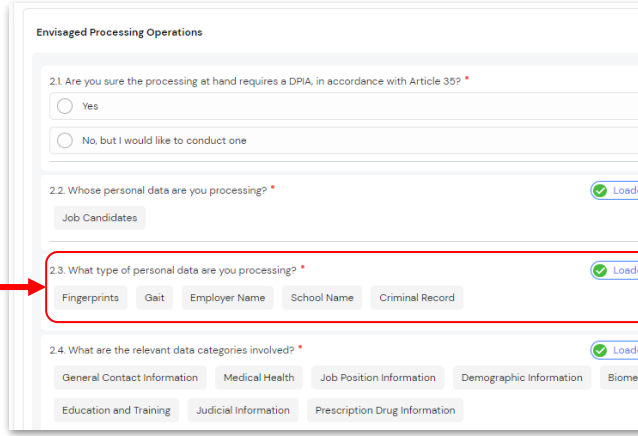
Fully automated report of Data subjects Vulnerability

and PII Sensitive

PIA integrated with RoPA

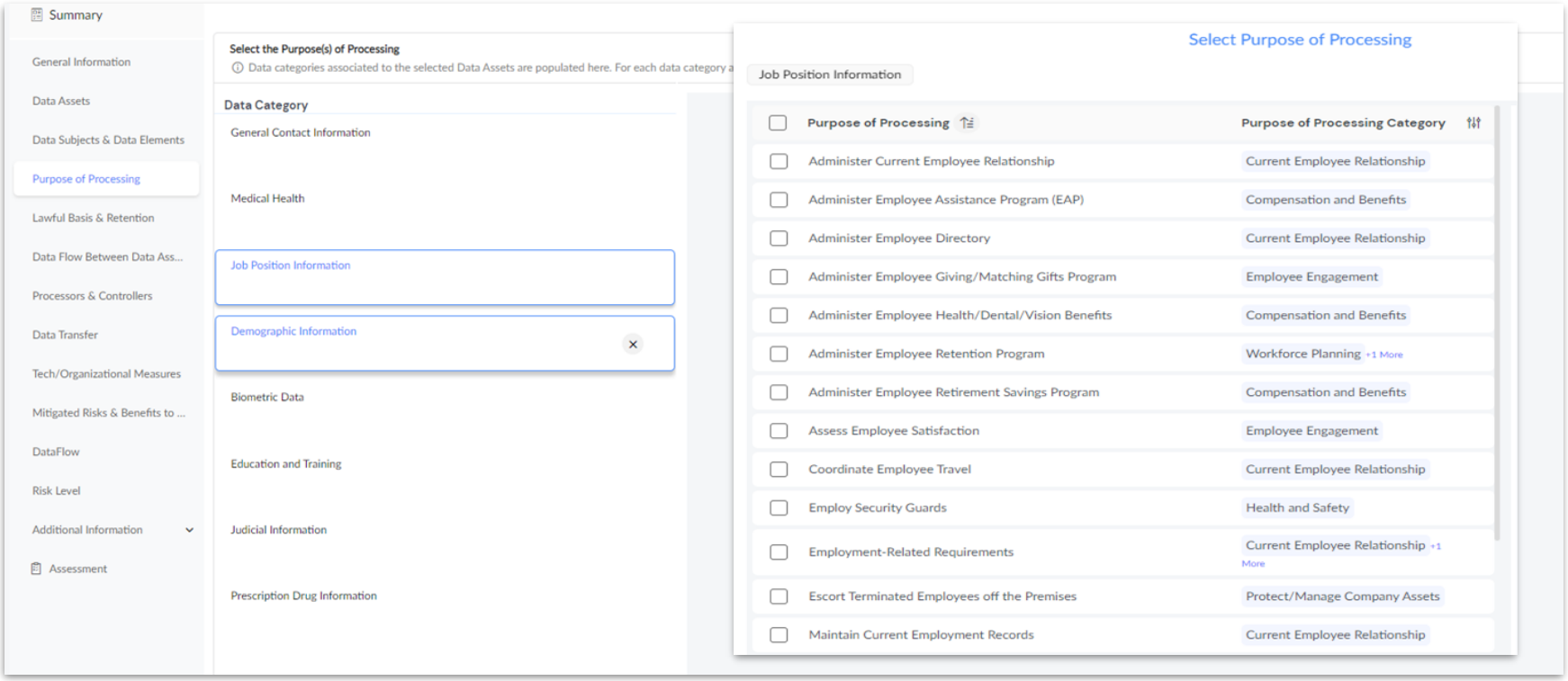
RoPA captures granular detail on Data Subjects and Data Elements, and it's automatically synced with the PIA, reducing time to answering redundant questions.





PIA integrated with RoPA

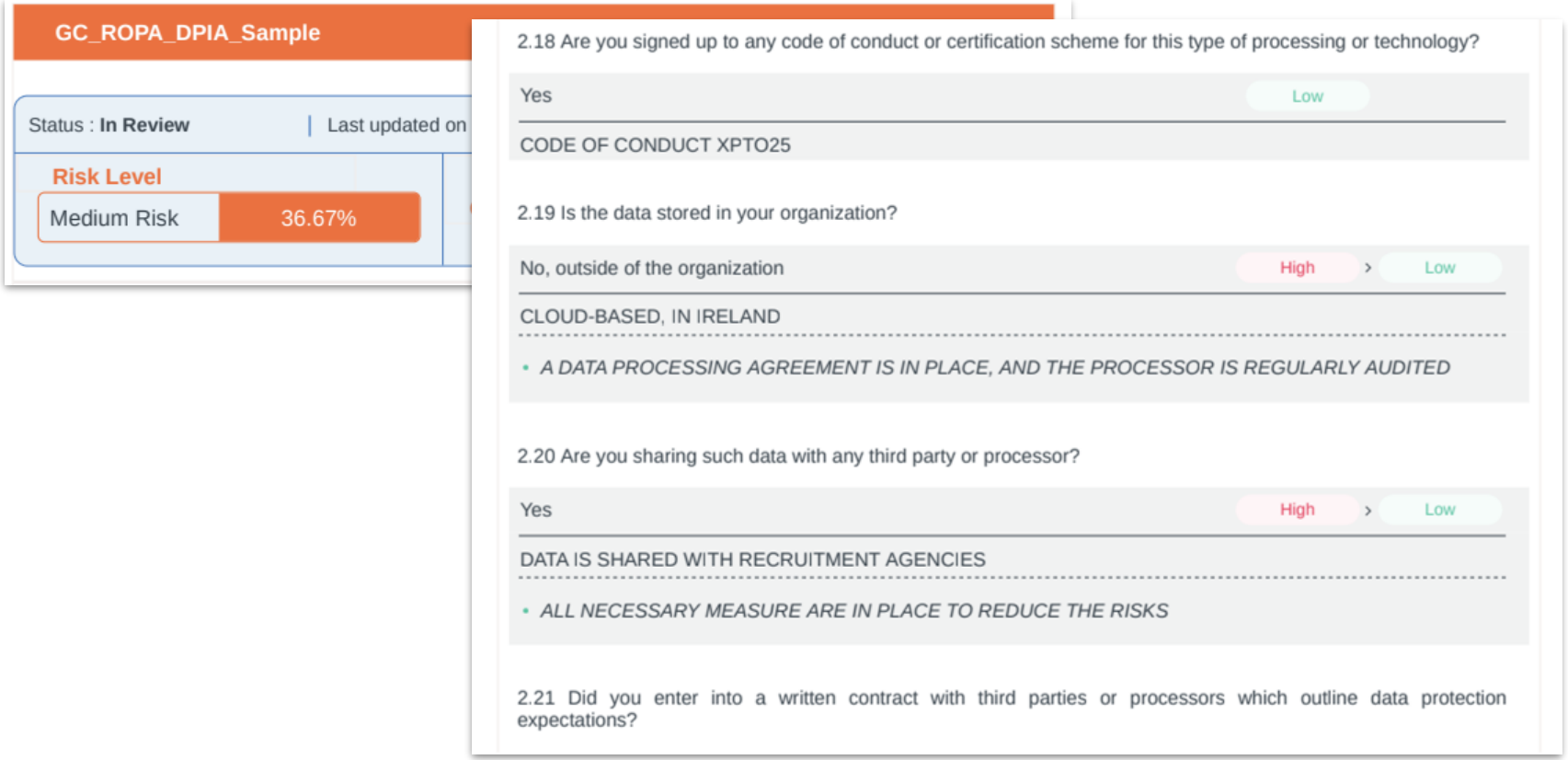
Captures granular detail on Data category, including the purpose for processing each data category.



Automatic risk level, allow for easy risk resolution

exterro ankura

SQUIRE PATTON BOGGS



Remediation

1. Develop a process and timeline for remediating risks.
    a) Some remediation activities need to be completed prior to engaging in the activity, such as:
        i. Encrypting data
        ii. Ensuring the system can delete data
        iii. Adding human involvement to an automated process
    b) Other risks need to be completed after engaging in the activity, such as:
        i. Conducting penetration tests on a system
        ii. Implementing de identification strategies
        iii. Audit of vendor security risk
2. Document status of remediation activities and be sure to check in at the appropriate timelines
3. Make sure you have an approval process that allows you to track the approval status over time

Confirm Reporting Approach

1. Consider in advance what information you want to share with a regulator/government agency.
2. Determine the format and amount of information that will be included and develop templates so that you are ready to comply with requests.
3. Consider which parts of the process you want to remain privileged and who will have access to and input on the legal conclusions that are made in the privacy risk review.

Constitutional Questions

The Free Speech / Privacy Conflict

- Sorrell (564 US 2634 (2011))
  - Collection and selling personal data is protected speech
- Zauder (471 US 626 (1985))
  - Deference for factual disclosures in advertising
- Netchoice (113 F.4th 1101(9th Cir. 2024)) and X Corp (2024 WL 4033063 (9th Cire 2024))
  - Content transparency and risk assessments are subject to strict scrutiny
- National Ass'n of Mfrs v SEC (DC Cir. 2015)
  - SEC disclosures are not advertising
  - But are commercial speech subject to intermediate scrutiny
- Beyond DPIAs

What Price Privacy?

While policy debate rages, the cost to business is clear

- Goldman, *Zauderer and Compelled Editorial Transparency*, 108 Iowa L. Rev Online 80 (2023)
- Balkin, *Information Fiduciaries and the First Amendment*, 49 UC Davis L. Rev 1183 (2016)
- Bambauer, The Relationships Between Speech and Conduct, 49 UC Davis L. Rev 1943 (2016)
- CPPA's Reg Impact Assessments on draft regs:
  - Over $4 Billion in implementation costs in year 1
  - $31 Billion loss of investments
  - $50 Billion reduction in current output
  - Loss of 98,000 FTE
  - Gross state product loss of $27 Billion

Key Takeaways

1. Create a data privacy inventory
2. Understand the regulations in scope for your company
3. Develop a workflow for completing PIAs
4. Create PIA assessment templates based on your regulatory scope
5. Complete PIAs and review for accuracy and risk, remediating risks as needed
6. Develop reporting template for submitting to government agencies

Questions?

CLE and IAPP Credit Reminder

ANA will manage CLE credits. New York practioners need to check in and out to qualify

You may seek IAPP educational credit for this program via the IAPP website.

Subscribe to the Privacy World Blog at https://www.privacyworld.blog/subscribe/ **or using this QR code**

APPENDIX

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.