SQUIRE
PATTON BOGGS

ankura

Data Risk Assessments - Artificial Intelligence and Privacy Impact Assessments

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

June 26th - 11:40 am to 12:20 pm

CLE and IAPP Credit

For those of you who require CLE credits please note the following states are approved or pending CLE for 1.00 general hour in AZ, CA, CT, NJ and NY.

After today's session you will receive a Uniform Certificate of Attendance to complete and email to our colleague Robin Hallagan at robin.hallagan@squirepb.com. Please make sure to add code **Priv1018.**

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

Subscribe to the Privacy World Blog: https://www.privacyworld.blog/subscribe/

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

Squire Patton Boggs

Sasha Kiosse

Associate

Sasha.kiosse@squirepb.com

+212.872.9610

- Associate, SPB's Data Privacy, Cybersecurity and Digital Assets Practice
- New York

Ankura Consulting

Colleen Yushchak

Senior Managing Director

colleen.yushchak@ankura.com

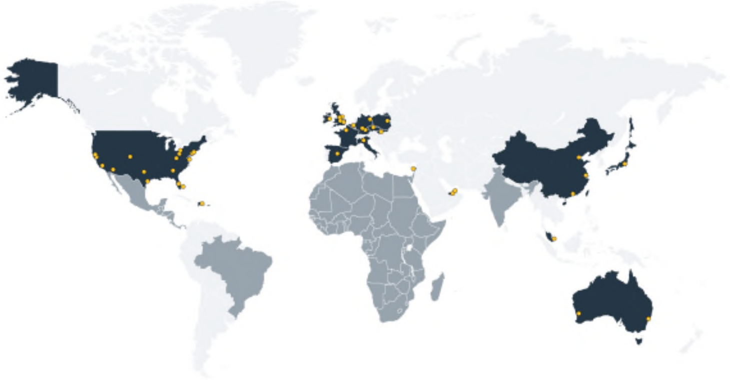
+202.361.8136

- Global Data Privacy Practice Leader
- Washington, D.C.

We are where you are

Over 40 Offices Across Four Continents

Ranked "Elite" Global Top 20 by Global Data Review 2022, 2023 & 2024 "Quick, pragmatic and business-savvy advice." Learn more here.



Abu Dhabi
Amsterdam
Atlanta
Beijing
Beirut
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Cincinnati
Cleveland
Columbus
Dallas
Denver

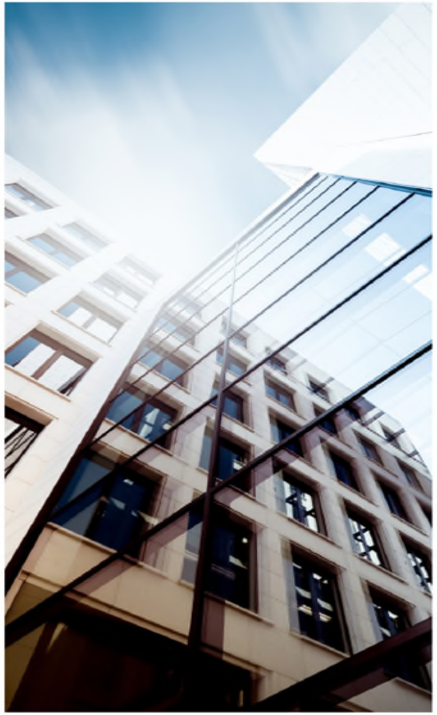
Dubai
Dublin
Frankfurt
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid
Manchester
Miami
Milan
New Jersey
New York

Palo Alto
Paris
Perth
Phoenix
Prague
San Francisco
Santo Domingo
Shanghai
Singapore
Sydney
Tampa
Tokyo
Warsaw
Washington DC

Africa
Brazil
Caribbean/Central America
India
Israel
Mexico

🟩 Office locations

■ Regional desks and strategic alliances



ankura

PROTECT, CREATE, AND RECOVER VALUE

WE PROACTIVELY IDENTIFY AND MITIGATE DATA PRIVACY RISKS, delivering practical solutions to meet the needs of business operations and industry trends.

WE LEAD PRIVACY PROGRAMS WITH A GLOBAL TEAM of highly credentialed and deeply experienced professionals that provide valuable insight to our clients every step of the way.

WE COLLABORATE WITH KEY INTERNAL STAKEHOLDERS AND EXTERNAL RESOURCES, such as outside counsel and technology vendors, to ensure privacy modernization programs are effective and sustainable.

DATA PRIVACY ASSESSMENT AND ROADMAP DEVELOPMENT

Assessment Using NIST Privacy Framework or Other Recognized Control Framework | Roadmap Development | Budgeting | Risk Mitigation

PRIVACY RIGHTS REQUEST PROCESS

Protocol and Procedures | Inquiry Intake Processes | Technology Automation Implementation and Support

NOTICES, POLICIES, AND PROCEDURES

Privacy Policies | Procedures for Employees | Operationalizing Policies and Procedures | Training | Process Development

DATA MAPPING AND PRIVACY IMPACT ASSESSMENTS

Data Mapping | Data Inventories | Privacy Impact Assessments | Risk Assessment and Mitigation | Technology and Process Enablement

RECORDS MANAGEMENT AND DATA DELETION PROGRAMS

Modernize Records Management Policy and Schedule | Operationalize Schedule and Implement Data Deletion Program | Leverage Technology to Support Scanning and Identification

PRIVACY SOLUTIONS ARCHITECTURE: DATA PRIVACY TECHNOLOGY IMPLEMENTATION SUPPORT

Advisory Oversight | Project Management Support | Technology Implementation

Agenda

1. **The purposes for and history of data practices assessments**

1. **U.S. state privacy laws' requirements for assessments.**

2. **A.I. Impact Assessment** – How to extend privacy impact assessments to include questions to support ethical A.I. governance.

3. **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.

1. **Take aways and Q&A**

SQUIRE PATTON BOGGS

ankura

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 Profiling**
- **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.

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

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.

CA AADA

If it passes Constitutional challenge:

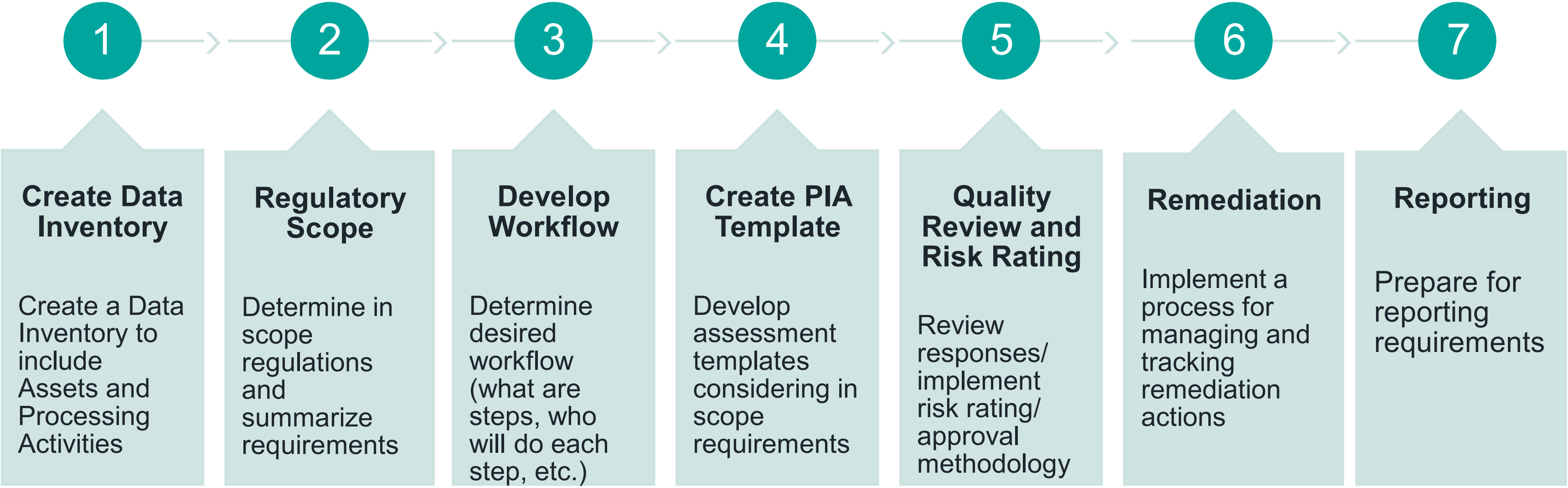
- The CAAADCA requires a DI&A:
  - identify the purpose of the online service, product, or feature,
  - describe how it uses Minors' Personal Data, and
  - discuss the risks of material detriment to Minors that arise from the data management practices.
- The DI&A must also address the, to the extent applicable, 8 specific questions.

SQUIRE PATTON BOGGS

ankura

Operationalizing Privacy and AI Impact Assessments

Steps to Operationalize Privacy and AI Impact Assessments



1. **Create Data Inventory**

   Create a Data Inventory to include Assets and Processing Activities

2. **Regulatory Scope**

   Determine in scope regulations and summarize requirements

3. **Develop Workflow**

   Determine desired workflow (what are steps, who will do each step, etc.)

4. **Create PIA Template**

   Develop assessment templates considering in scope requirements

5. **Quality Review and Risk Rating**

   Review responses/ implement risk rating/ approval methodology

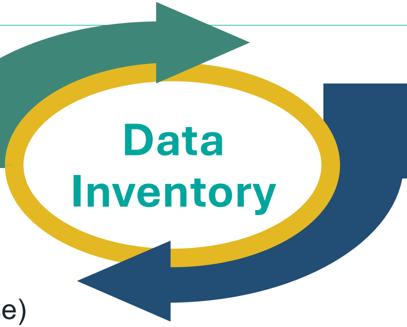
6. **Remediation**

   Implement a process for managing and tracking remediation actions

7. **Reporting**

   Prepare for reporting requirements

Step 1: Create Data Inventory



Data Inventory

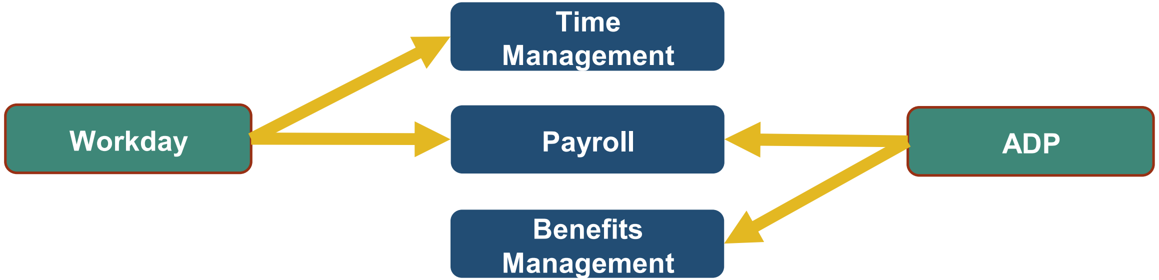
Asset Assessments

- An **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.*

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



Workday

Time Management

Payroll

Benefits Management

ADP

Step 2: Determine Regulatory Requirements in Scope

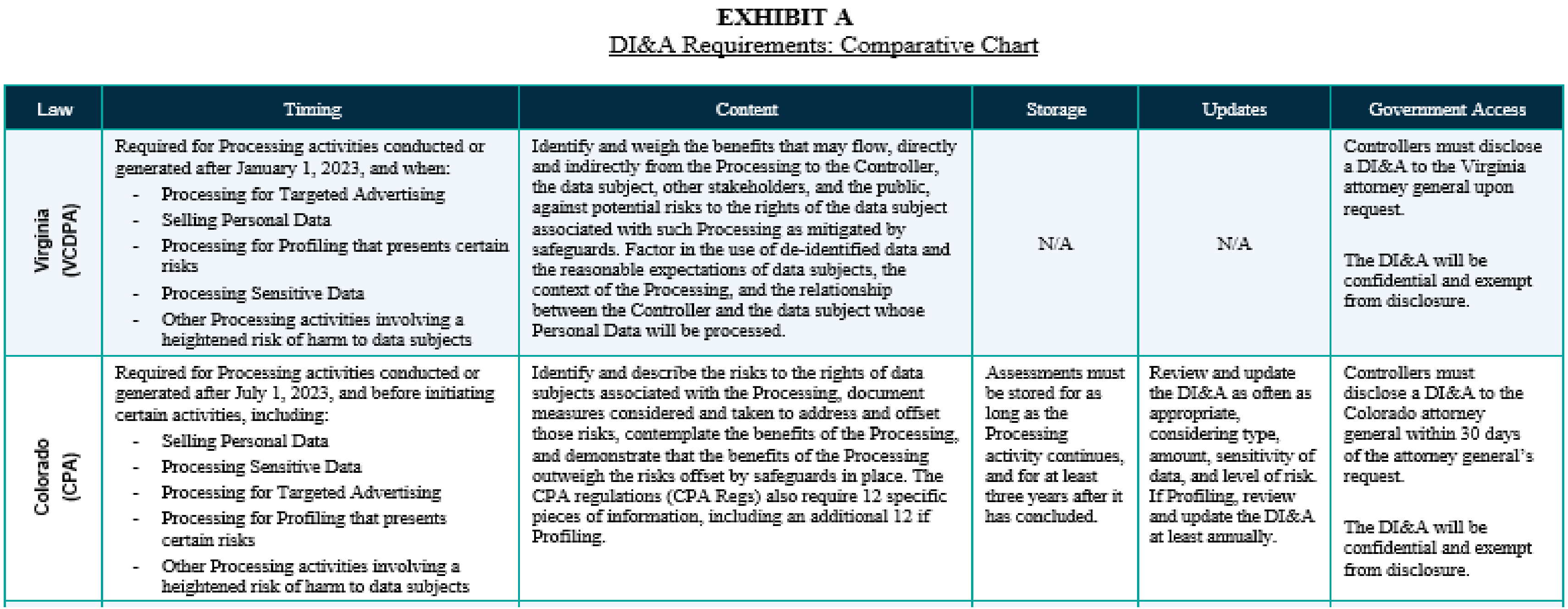


EXHIBIT A

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.

SPB and Ankura have developed a Data Inventory and Assessment Guidance and Templates toolkit that details requirements for all state privacy and AI laws.

Step 2: Determine Regulatory Requirements in Scope

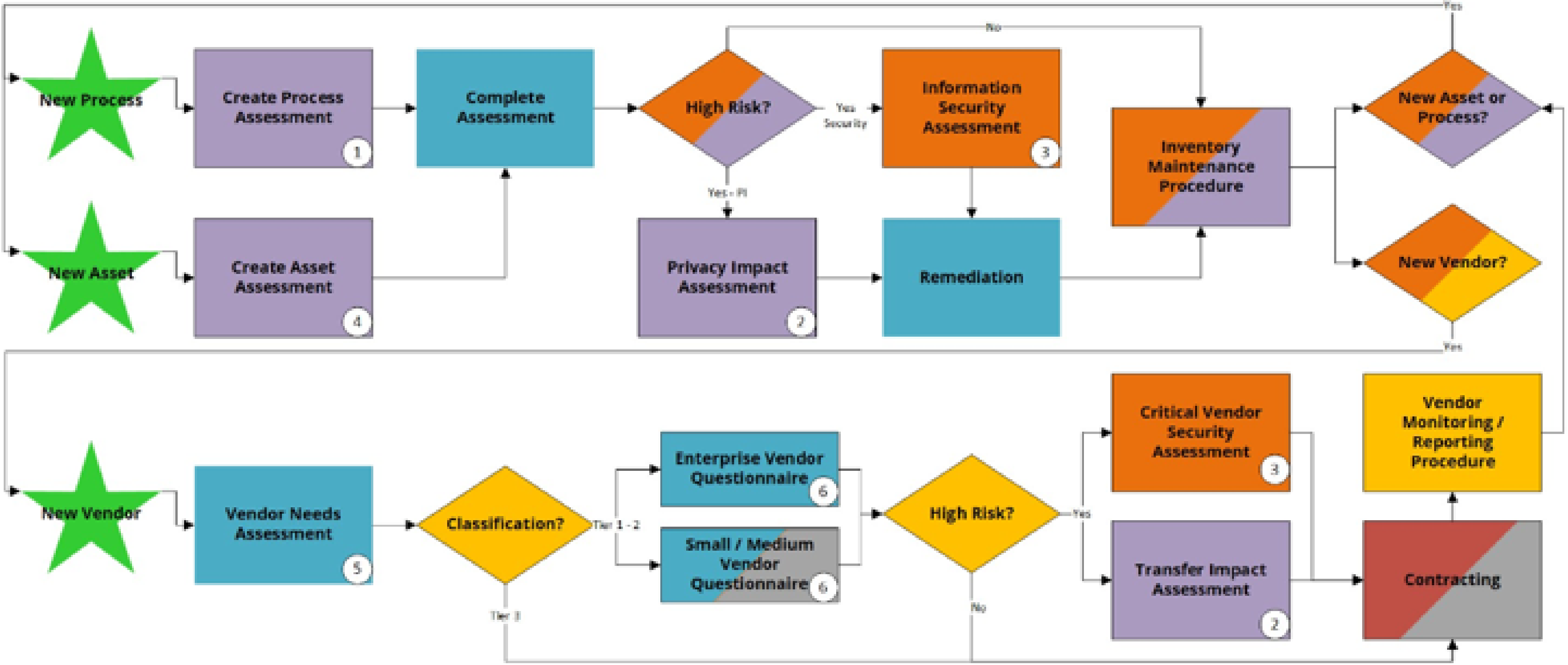
Consider Separate Questions or Assessment to Assess AI Activities (examples below):

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

Responsible Party

🟦 Business Owner 🟨 Vendor Risk 🟪 Privacy Office 🟧 Information Security 🟥 Legal ⬜ Vendor



New Process

Create Process Assessment 1

Complete Assessment

High Risk?

Yes - Security

No

Information Security Assessment 3

Inventory Maintenance Procedure

New Asset or Process?

Yes

New Asset

Create Asset Assessment 4

Yes - PI

Privacy Impact Assessment 2

Remediation

New Vendor?

Yes

New Vendor

Vendor Needs Assessment 5

Classification?

Tier 1 - 2

Tier 3

Enterprise Vendor Questionnaire 6

Small / Medium Vendor Questionnaire 6

High Risk?

Yes

No

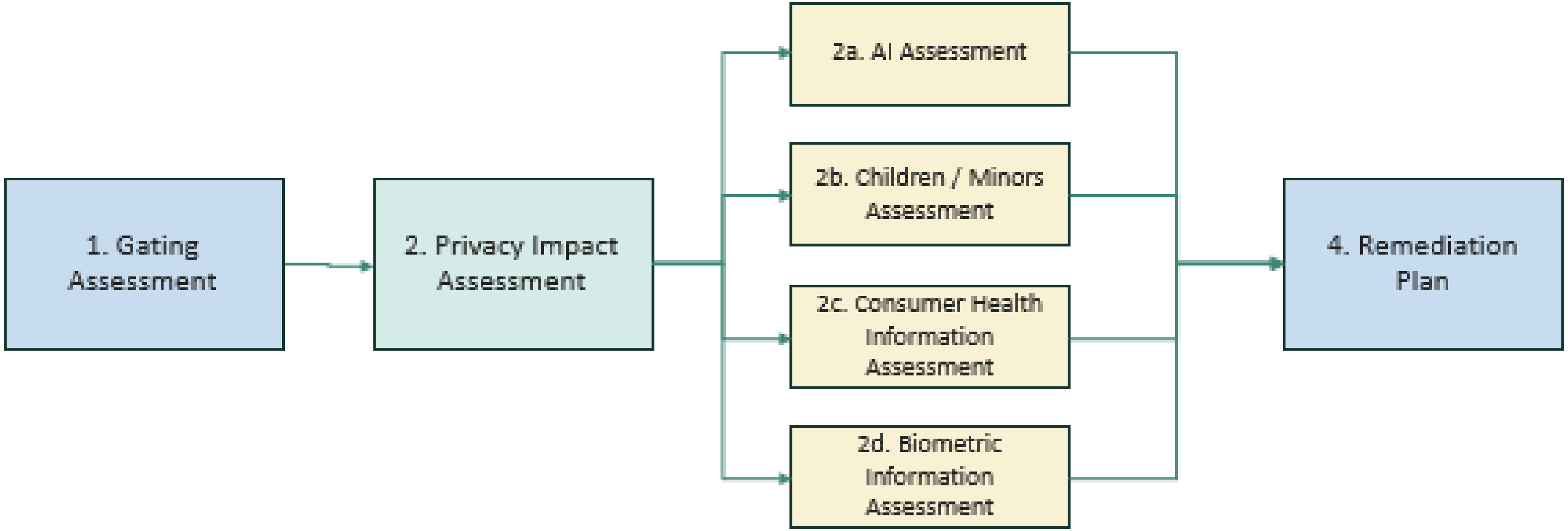
Critical Vendor Security Assessment 3

Transfer Impact Assessment 2

Vendor Monitoring / Reporting Procedure

Contracting

Step 3: Determine Desired Workflow

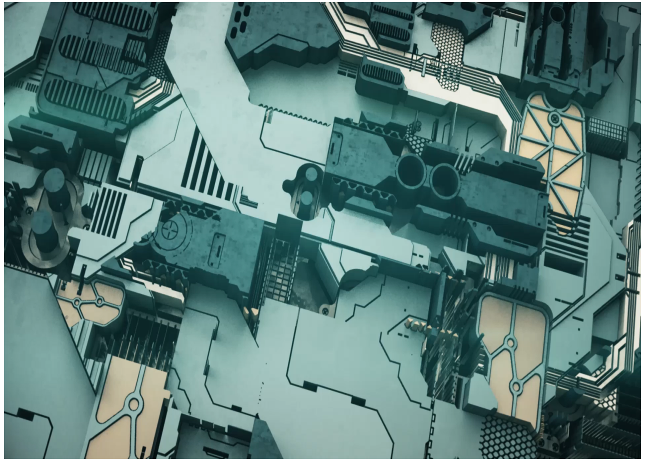

1. Gating Assessment
2. Privacy Impact Assessment
2a. AI Assessment
2b. Children / Minors Assessment
2c. Consumer Health Information Assessment
2d. Biometric Information Assessment
4. Remediation Plan

Step 4: Develop PIA Template

Consider Using Privacy Management Technology

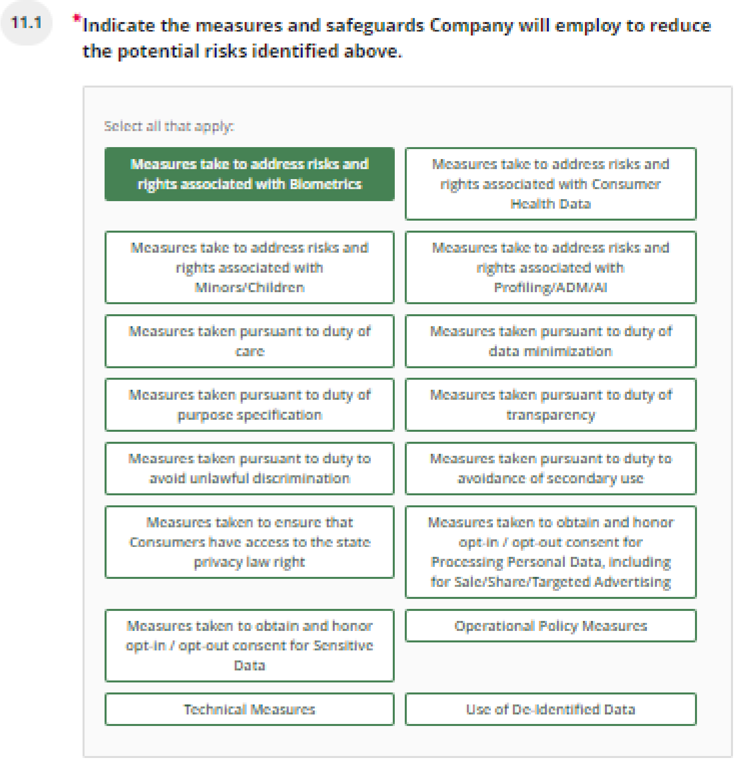
Benefits Include:

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 PIA in OneTrust

Conditional Logic Example: If we select the “biometric” button below:



11.1 *Indicate the measures and safeguards Company will employ to reduce the potential risks identified above.

Select all that apply:

☑ Measures take to address risks and rights associated with Biometrics

□ Measures take to address risks and rights associated with Consumer Health Data

□ Measures take to address risks and rights associated with Minors/Children

□ Measures take to address risks and rights associated with Profiling/ADM/AI

□ Measures taken pursuant to duty of care

□ Measures taken pursuant to duty of data minimization

□ Measures taken pursuant to duty of purpose specification

□ Measures taken pursuant to duty of transparency

□ Measures taken pursuant to duty to avoid unlawful discrimination

□ Measures taken pursuant to duty to avoidance of secondary use

□ Measures taken to ensure that Consumers have access to the state privacy law right

□ Measures taken to obtain and honor opt-in / opt-out consent for Processing Personal Data, including for Sale/Share/Targeted Advertising

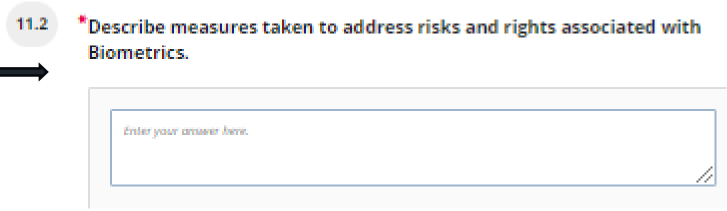
□ Measures taken to obtain and honor opt-in / opt-out consent for Sensitive Data

□ Operational Policy Measures

□ Technical Measures

□ Use of De-Identified Data

..that prompts an additional follow-up question which appears below question 11.1 →



11.2 *Describe measures taken to address risks and rights associated with Biometrics.

Enter your answer here.

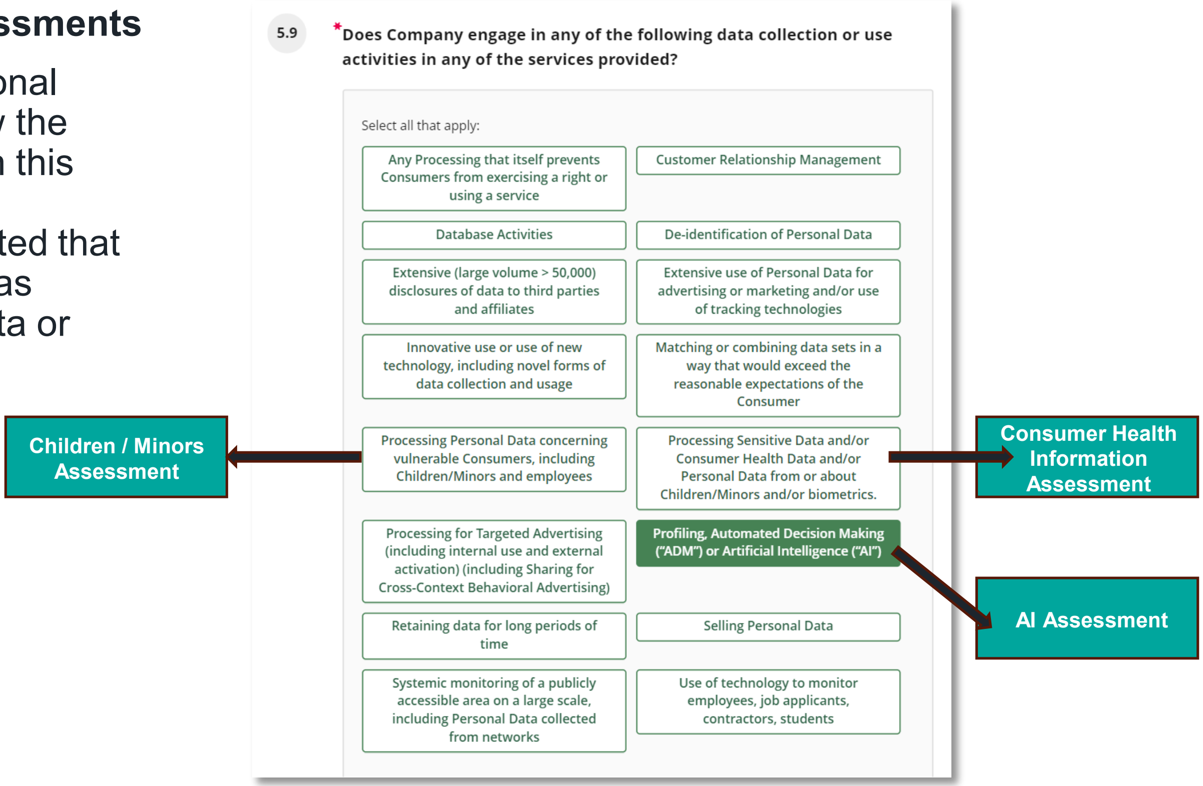
Step 4: Examples of PIA in OneTrust

ankura

SQUIRE PATTON BOGGS

Use Rules to Launch New Assessments

We can use rules to launch additional questionnaires, depending on how the respondent answers questions. In this case, we can launch separate assessments if an activity is selected that requires additional controls, such as Children / Minors Data, Health Data or Artificial Intelligence.



5.9 *Does Company engage in any of the following data collection or use activities in any of the services provided?

Select all that apply:

Any Processing that itself prevents Consumers from exercising a right or using a service

Customer Relationship Management

Database Activities

De-identification of Personal Data

Extensive (large volume > 50,000) disclosures of data to third parties and affiliates

Extensive use of Personal Data for advertising or marketing and/or use of tracking technologies

Innovative use or use of new technology, including novel forms of data collection and usage

Matching or combining data sets in a way that would exceed the reasonable expectations of the Consumer

Processing Personal Data concerning vulnerable Consumers, including Children/Minors and employees

Processing Sensitive Data and/or Consumer Health Data and/or Personal Data from or about Children/Minors and/or biometrics.

Processing for Targeted Advertising (including internal use and external activation) (including Sharing for Cross-Context Behavioral Advertising)

[✓ Profiling, Automated Decision Making (“ADM”) or Artificial Intelligence (“AI”)]

Retaining data for long periods of time

Selling Personal Data

Systemic monitoring of a publicly accessible area on a large scale, including Personal Data collected from networks

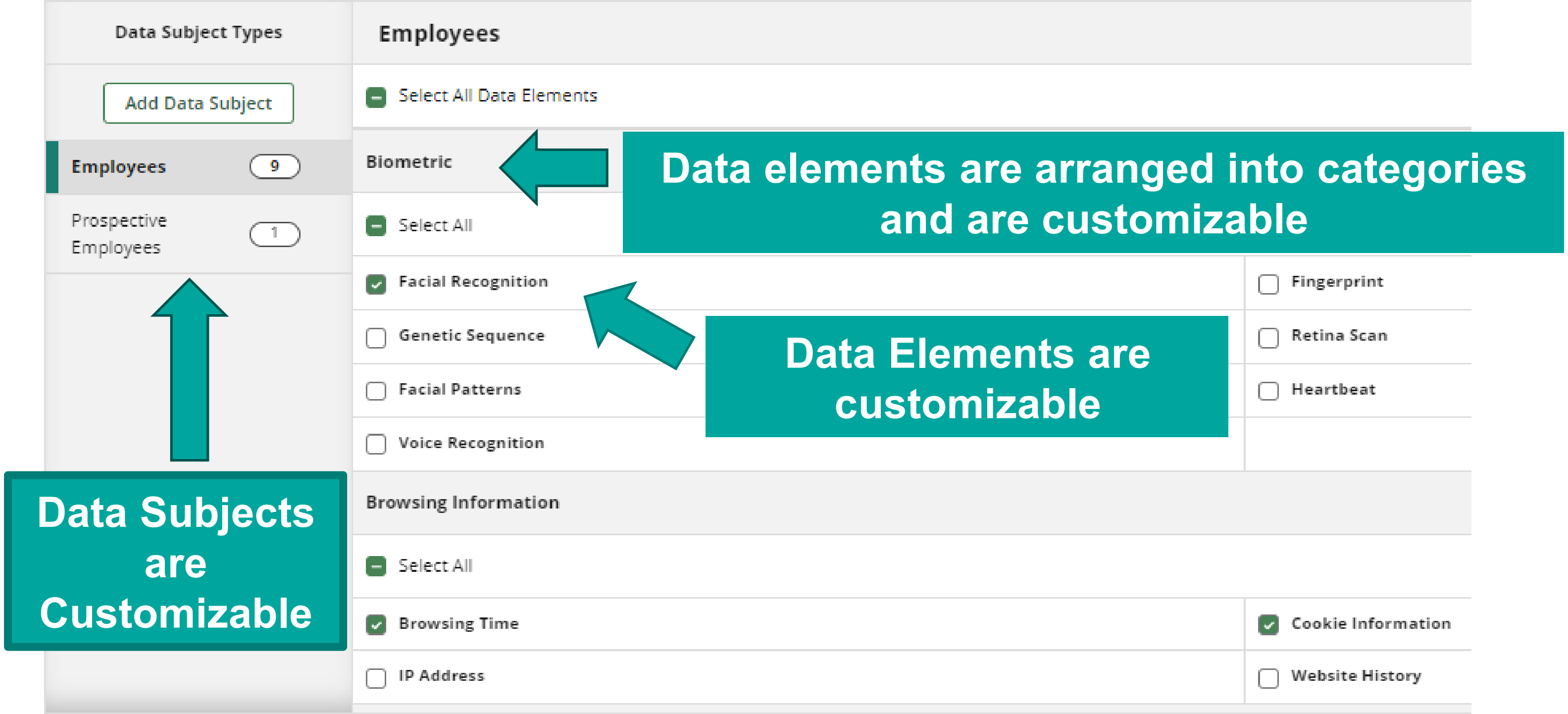
Use of technology to monitor employees, job applicants, contractors, students

Children / Minors Assessment
Consumer Health Information Assessment
AI Assessment

Step 4: Examples of PIA in OneTrust

ankura SQUIRE PATTON BOGGS

Captures granular detail on Data Subjects/Categories of Data/Data Elements



Data Subject Types

Add Data Subject

Employees 9

Prospective Employees 1

Employees

▬ Select All Data Elements

Biometric

▬ Select All

☑ Facial Recognition	□ Fingerprint
□ Genetic Sequence	□ Retina Scan
□ Facial Patterns	□ Heartbeat
□ Voice Recognition	

Browsing Information

▬ Select All

☑ Browsing Time	☑ Cookie Information
□ IP Address	□ Website History

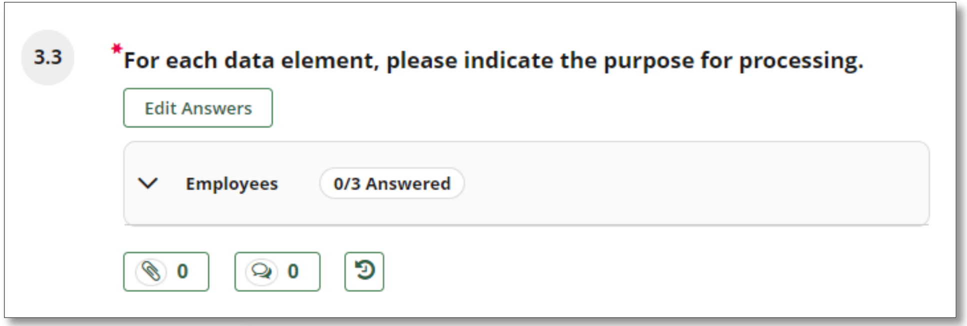
Data elements are arranged into categories and are customizable

Data Elements are customizable

Data Subjects are Customizable

Step 4: Examples of PIA in OneTrust

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

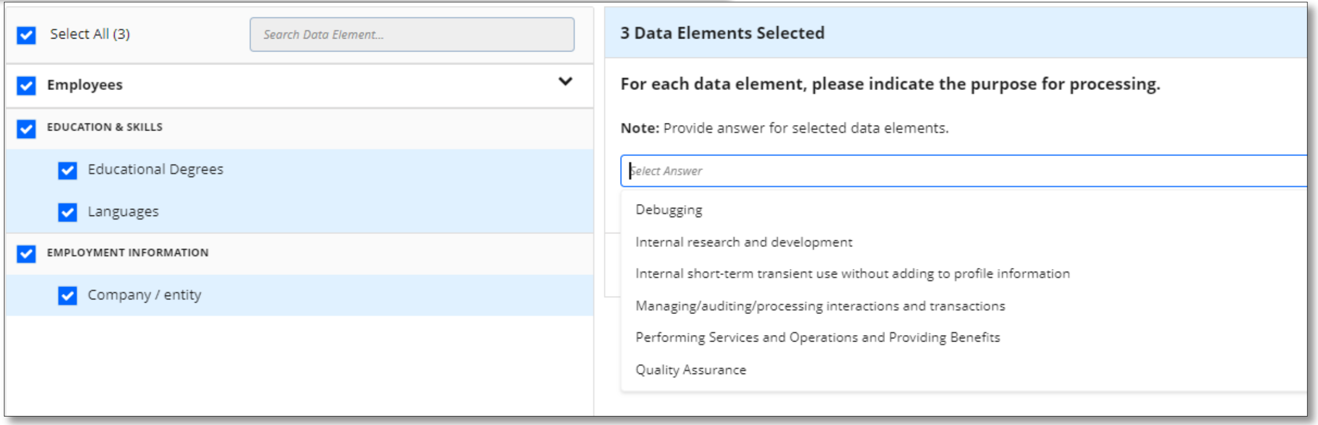


3.3 *For each data element, please indicate the purpose for processing.

Edit Answers

Employees 0/3 Answered

0 0



☑ Select All (3) Search Data Element...

☑ Employees

☑ EDUCATION & SKILLS

☑ Educational Degrees

☑ Languages

☑ EMPLOYMENT INFORMATION

☑ Company / entity

3 Data Elements Selected

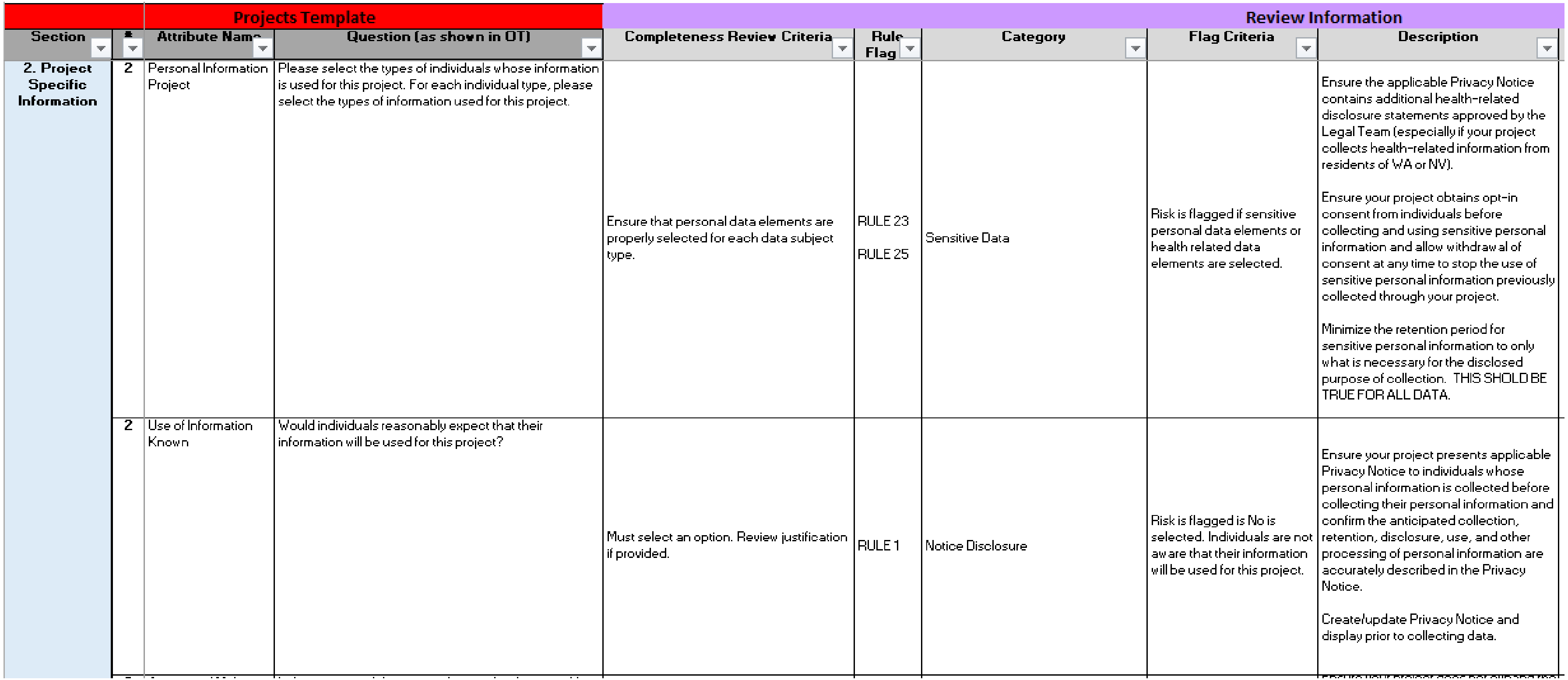
For each data element, please indicate the purpose for processing.

Note: Provide answer for selected data elements.

Select Answer

- Debugging
- Internal research and development
- Internal short-term transient use without adding to profile information
- Managing/auditing/processing interactions and transactions
- Performing Services and Operations and Providing Benefits
- Quality Assurance

Step 5: Develop Quality Review and Risk Rating Approach



		Projects Template		Review Information				
Section	#	Attribute Nam	Question (as shown in OT)	Completeness Review Criteria	Rule Flag	Category	Flag Criteria	Description
2. Project Specific Information	2	Personal Information Project	Please select the types of individuals whose information is used for this project. For each individual type, please select the types of information used for this project.	Ensure that personal data elements are properly selected for each data subject type.	RULE 23 RULE 25	Sensitive Data	Risk is flagged if sensitive personal data elements or health related data elements are selected.	Ensure the applicable Privacy Notice contains additional health-related disclosure statements approved by the Legal Team (especially if your project collects health-related information from residents of WA or NV). Ensure your project obtains opt-in consent from individuals before collecting and using sensitive personal information and allow withdrawal of consent at any time to stop the use of sensitive personal information previously collected through your project. Minimize the retention period for sensitive personal information to only what is necessary for the disclosed purpose of collection. THIS SHOLD BE TRUE FOR ALL DATA.
	2	Use of Information Known	Would individuals reasonably expect that their information will be used for this project?	Must select an option. Review justification if provided.	RULE 1	Notice Disclosure	Risk is flagged is No is selected. Individuals are not aware that their information will be used for this project.	Ensure your project presents applicable Privacy Notice to individuals whose personal information is collected before collecting their personal information and confirm the anticipated collection, retention, disclosure, use, and other processing of personal information are accurately described in the Privacy Notice. Create/update Privacy Notice and display prior to collecting data.

Step 6: 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. Conducing penetration tests on a system
      ii. Implementing deidentification 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

Step 7: 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.

Shortcut to Compliance

SPB and Ankura's Data Inventory and Assessment Guidance and Templates Toolkit contains:

1. Chart comparing laws that require assessments
2. Assessment quick guidance check list with instructions and detailed guidance on how to complete assessments (SPB clients only)
3. Full Templates (*can be licensed to outside of legal services*):
    1. Data inventory and assessment template including gating assessment, assessment and material changes.
    2. AI and ADM/Profiling supplement
    3. Children's/minors supplement
    4. Consumer health data supplement
    5. Biometric data supplement
4. Data practices assessments guidance document (SPB clients only)
5. Guidance on developing and maintaining an information governance program (SPB clients only)
6. Template company policy on conducting assessments (SPB clients only)

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

Thank you & Questions?

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

Squire Patton Boggs

Sasha Kiosse

Associate

Sasha.kiosse@squirepb.com

+212.872.9610

- Associate, SPB's Data Privacy, Cybersecurity and Digital Assets Practice
- New York

Ankura Consulting

Colleen Yushchak

Senior Managing Director

colleen.yushchak@ankura.com

+202.361.8136

- Global Data Privacy Practice Leader
- Washington, D.C.

CLE and IAPP Credit Reminder

For those of you who require CLE credits please note the following states are approved or pending CLE for 1.00 general hour in AZ, CA, CT, NJ and NY.

After today’s session you will receive a Uniform Certificate of Attendance to complete and email to our colleague Robin Hallagan at robin.hallagan@squirepb.com. Please make sure to add code **Priv1018.**

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

Subscribe to the Privacy World Blog: https://www.privacyworld.blog/subscribe/