SQUIRE PATTON BOGGS

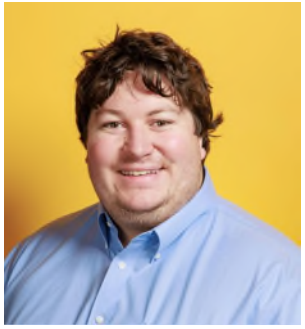
Local Connections.
Global Influence.

Dino-Mitigation Plan: AI Risk Assessments and Compliance Obligations

Contacts

SQUIRE PATTON BOGGS

Kyle R. Dull
Senior Associate
Squire Patton Boggs (US) LLP
Kyle.Dull@squirepb.com



Daniel McVay
CIPP/US/C, CIPM, AIGP
Corporate Counsel Product Privacy, LCPO
Intuit
Daniel_McVay@intuit.com

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

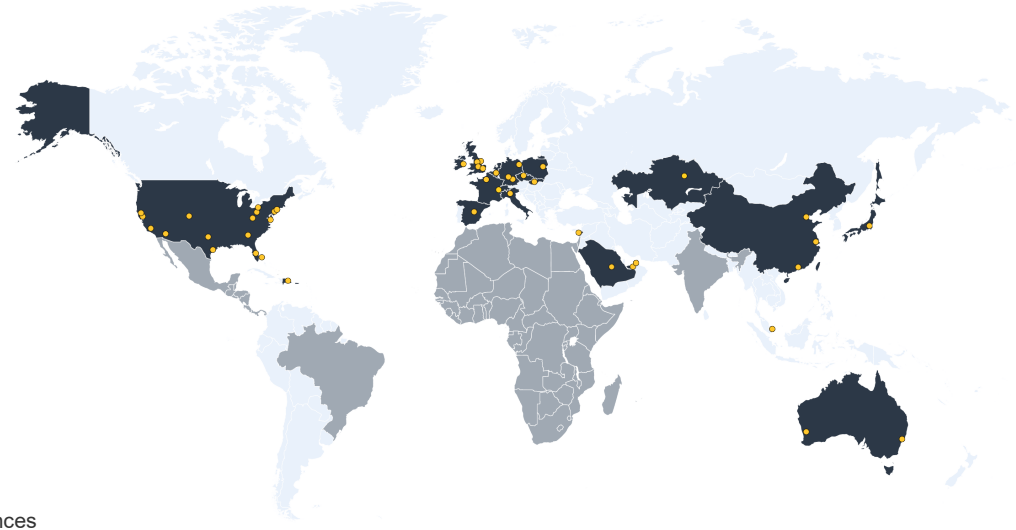
Subscribe to the Privacy World Blog:
https://www.privacyworld.blog/subscribe/

SQUIRE PATTON BOGGS

Data Privacy, Cybersecurity and Digital Asset Team

Abu Dhabi
Amsterdam
Astana
Atlanta
Beijing
Beirut
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Cincinnati
Cleveland
Columbus
Dallas
Denver
Dubai
Dublin
Frankfurt
Geneva
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid
Manchester
Miami
Milan
New Jersey
New York
Palo Alto
Paris
Perth
Phoenix
Prague
Riyadh
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

80 Data Lawyers in 14 Countries…

SQUIRE PATTON BOGGS

- Approximately 80 lawyers in our Data Privacy, Cybersecurity and Digital Assets Group
  - Teams located throughout the US, UK, Europe, Middle East, and Asia.
  - Includes former enforcement attorneys and prosecutors and in-house counsel.
  - We recently welcomed back Lydia de la Torre who returned to the firm after having served as an inaugural board member of the California Privacy Protection Agency (responsible for the CCPA regulations).

Session Outline

SQUIRE PATTON BOGGS

How did we get here?

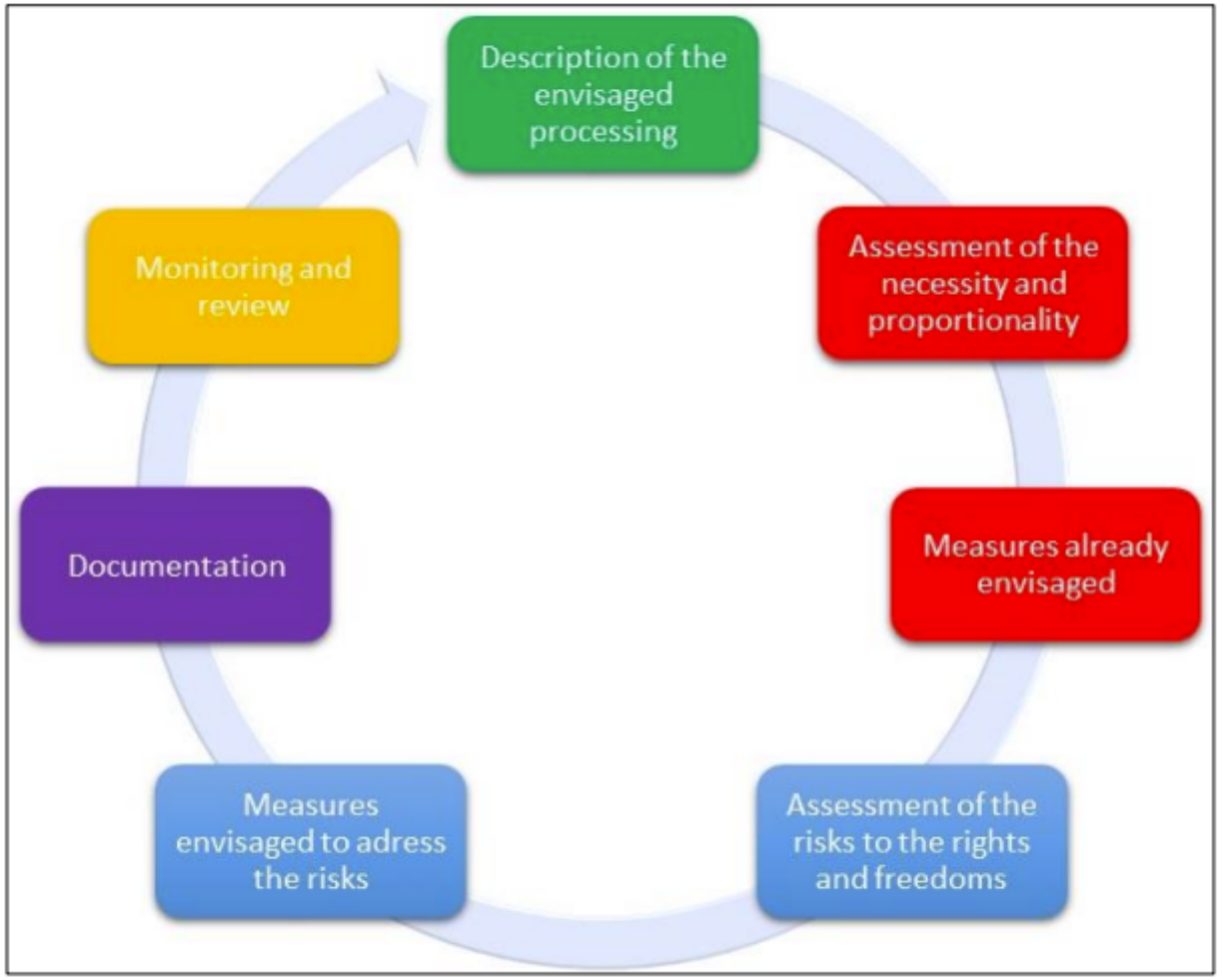
The purposes for and history of data practices assessments

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

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

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.

Take aways and Q&A


Description of the envisaged processing
Assessment of the necessity and proportionality
Measures already envisaged
Assessment of the risks to the rights and freedoms
Measures envisaged to adress the risks
Documentation
Monitoring and review

SQUIRE PATTON BOGGS

Europe + State Consumer Privacy Laws

20 States + AI and other AI related Laws

	State	Consumer Privacy Law Title	Effective Date
1.	California	California Consumer Privacy Act, as amended by the California Privacy Rights Act (CPRA) (collectively, CCPA)	Initial CCPA Effective Date: January 1, 2020 CPRA amendments Effective Date: January 1, 2023
2.	Colorado	Colorado Privacy Act (CO-CPA)	July 1, 2023
3.	Connecticut	Connecticut Data Privacy and Online Monitoring Act (CT-DPA)	July 1, 2023
4.	Delaware	Delaware Personal Data Privacy Act (DE-PDPA)	January 1, 2025
5.	Florida	Florida Digital Bill of Rights (FL-DBR)	July 1, 2024
6.	Indiana	Indiana Consumer Data Protection Act (IN-CDPA)	January 1, 2026
7.	Iowa	Act Relating to Consumer Data Protection (IA-CDPA)	January 1, 2025
8.	Kentucky	Act Relating to Consumer Data Privacy (KY-CDPA)	January 1, 2026
9.	Maryland	Maryland Online Data Privacy Act (MD-ODPA)	October 1, 2025
10.	Minnesota	Minnesota Consumer Data Privacy Act (MN-CDPA)	July 31, 2025*
11.	Montana	Montana Consumer Data Privacy Act (MT-CDPA)	October 1, 2024
12.	Nebraska	Data Privacy Act (NE-DPA)	January 1, 2025
13.	New Hampshire	Act Relative to the Expectation of Privacy (NH-PA)	January 1, 2025
14.	New Jersey	Act Concerning Online Services, Consumers, and Personal Data (NJ-DPA)	January 15, 2025
15.	Oregon	Oregon Consumer Privacy Act (OR-CPA)	July 1, 2024 **
16.	Rhode Island	Rhode Island Data Transparency and Privacy Protection Act (RI-DTPPA)	January 1, 2026
17.	Tennessee	Tennessee Information Protection Act (TN-IPA)	July 1, 2025
18.	Texas	Texas Data Privacy and Security Act (TX-DPSA)	July 1, 2024
19.	Utah	Utah Consumer Privacy Act (UT-CPA)	December 31, 2023
20.	Virginia	Virginia Consumer Data Protection Act (VA-CDPA)	January 1, 2023

What Organizations are in Scope?

SQUIRE PATTON BOGGS

- Usually based on a **Processing threshold of state residents** (35,000 to 100,000 (with lower thresholds if majority of revenue is based on the sale of personal information)) or a **global gross revenues** ($25m) (or a combination of both)
- Some state laws apply even if the controller Processes the personal information of one state resident
  - Texas
  - Nebraska

SQUIRE PATTON BOGGS

Assessments

Background

Assessments: Required v. Best Practice

SQUIRE PATTON BOGGS

- Identify and mitigate risk
- Keep RoPAs / data inventories / data mapping 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

When Are they Required?

SQUIRE PATTON BOGGS

- 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~~).

Processing Sensitive Data

SQUIRE PATTON BOGGS

- Personal information that reveals a consumer's:
  - Social security, drivers' license, state identification card, or passport number
  - Account log-in financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account
  - Precise geolocation
  - Racial or ethnic origin
  - Citizenship or immigration status
  - Religious or philosophical beliefs, or union membership
  - Contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication
  - Genetic data
- Biometric information (defined below) processed for the purpose of uniquely identifying a consumer
- Personal information collected and analyzed concerning a consumer's health
- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation

Targeted Advertising

SQUIRE PATTON BOGGS

- Displaying to a consumer an advertisement
- That is selected elected based on personal data obtained or inferred over time
- From the consumer's activities across non-affiliated websites, applications, or online services
- To predict a consumer's preferences or interests

Selling Personal Information

SQUIRE PATTON BOGGS

- selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.
- Doe not mean:
  - The disclosure of personal data when the consumer: (i) directs the controller to disclose the personal data; and (ii) intentionally uses the controller to interact with a third party
  - The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets

Processing Personal Data for **high-risk Profiling**

SQUIRE PATTON BOGGS

"Profiling" means any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's intelligence, ability, aptitude, performance at work, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements.

- Targeted advertising;
- Sales of personal data;
- Processing personal data for profiling which creates certain risks for consumers; and
- Processing sensitive data.

Profiling that has a **significant impact** on the data subject

SQUIRE PATTON BOGGS

- Significant impact that results in the access to, or the provision or denial of:
  - Financial or lending services
  - Housing
  - Insurance
  - Education enrollment or opportunity
  - Criminal justice
  - Employment or independent contracting opportunities or compensation
  - Healthcare services
  - Essential goods or services [e.g., groceries, medicine, hygiene products, or fuel]

Significant Decision/Impact

SQUIRE PATTON BOGGS

- Significant impact that results in the access to, or the provision or denial of:
  - Financial or lending services
  - Housing
  - Insurance
  - Education enrollment or opportunity
  - Criminal justice
  - Employment or independent contracting opportunities or compensation
  - Healthcare services
  - Essential goods or services [e.g., groceries, medicine, hygiene products, or fuel]
- Does not mean decisions subject to specific enumerated exceptions

Automated decision-making technology

SQUIRE PATTON BOGGS

- "Automated decisionmaking technology" means any technology that processes personal information and uses computation to
  - execute a decision,
  - replace human decisionmaking, or
  - substantially facilitate human decisionmaking.

AI

SQUIRE PATTON BOGGS

- “Artificial intelligence” means a machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments.
  - The artificial intelligence may do this to achieve explicit or implicit objectives.
  - Outputs can include predictions, content, recommendations, or decisions.
  - Different artificial intelligence varies in its levels of autonomy and adaptiveness after deployment.
- For example, artificial intelligence includes generative models, such as large language models, that can learn from inputs and create new outputs, such as text, images, audio, or video; and facial- or speech-recognition or-detection technology.

Additional Processing Activities Requiring an Assessment

SQUIRE PATTON BOGGS

1. Systemic and extensive evaluations based on automated Processing (EDPB and CA)
2. Processing data on a large scale (EPDB)
3. Processing the Personal Data of data subjects to train AI or ADM technology (CA Discussion Draft Regs).
4. 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).
5. Innovative use or use of new technology (EDPB)
6. Processing itself prevents data subjects from exercising a right or using a service (EDPB guidelines) (CA Discussion Draft Regs as to ADM)
7. Use of cookies or other tracking technologies
8. When a security incident would trigger an obligation to notify data subjects or the government (not explicitly required but recommended).

What Should Assessments Document?

SQUIRE PATTON BOGGS

- 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

Florida

(very limited definition of controller)

Florida

SQUIRE PATTON BOGGS

- A **controller** must conduct and document a data protection assessment for each of the following processing activities involving personal data that were generated on or after July 1, 2023:
  - Processing of personal data for purposes of targeted advertising.
  - Selling personal data.
  - Processing of personal data for purposes of profiling that presents a reasonably foreseeable risk of:
    - Unfair or deceptive treatment of consumers
    - Unlawful disparate impact on consumers
    - Financial, physical, or reputational injury to consumers
    - A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person
    - Other substantial injury to consumers
  - Processing of sensitive data
  - Any processing activities involving personal data which present a heightened risk of harm to consumers

SQUIRE PATTON BOGGS

Colorado

Colorado Privacy Act and the Colorado AI Act

Colorado Privacy Act

SQUIRE PATTON BOGGS

- 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

Colorado AI Act

SQUIRE PATTON BOGGS

- If it is not ultimately preempted 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

SQUIRE PATTON BOGGS

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

California

CCPA and More

CPPA Draft Regulations on Assessments

SQUIRE PATTON BOGGS

- 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**

Operational Elements of the Assessment

SQUIRE PATTON BOGGS

- 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.

Questions to Ask for AI Activities:

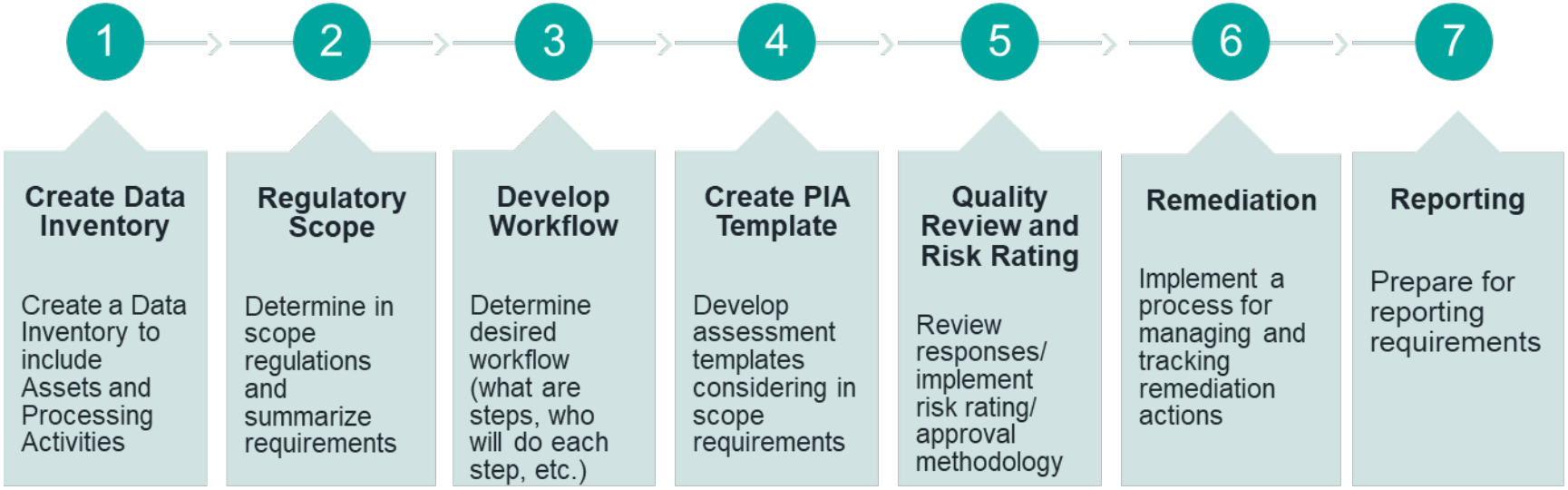
SQUIRE PATTON BOGGS

1. Describe all intended uses of the system / process.
2. Indicate whether there will be human involvement in the AI or ADM/Profiling process, including any appeals process.
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.

SQUIRE PATTON BOGGS

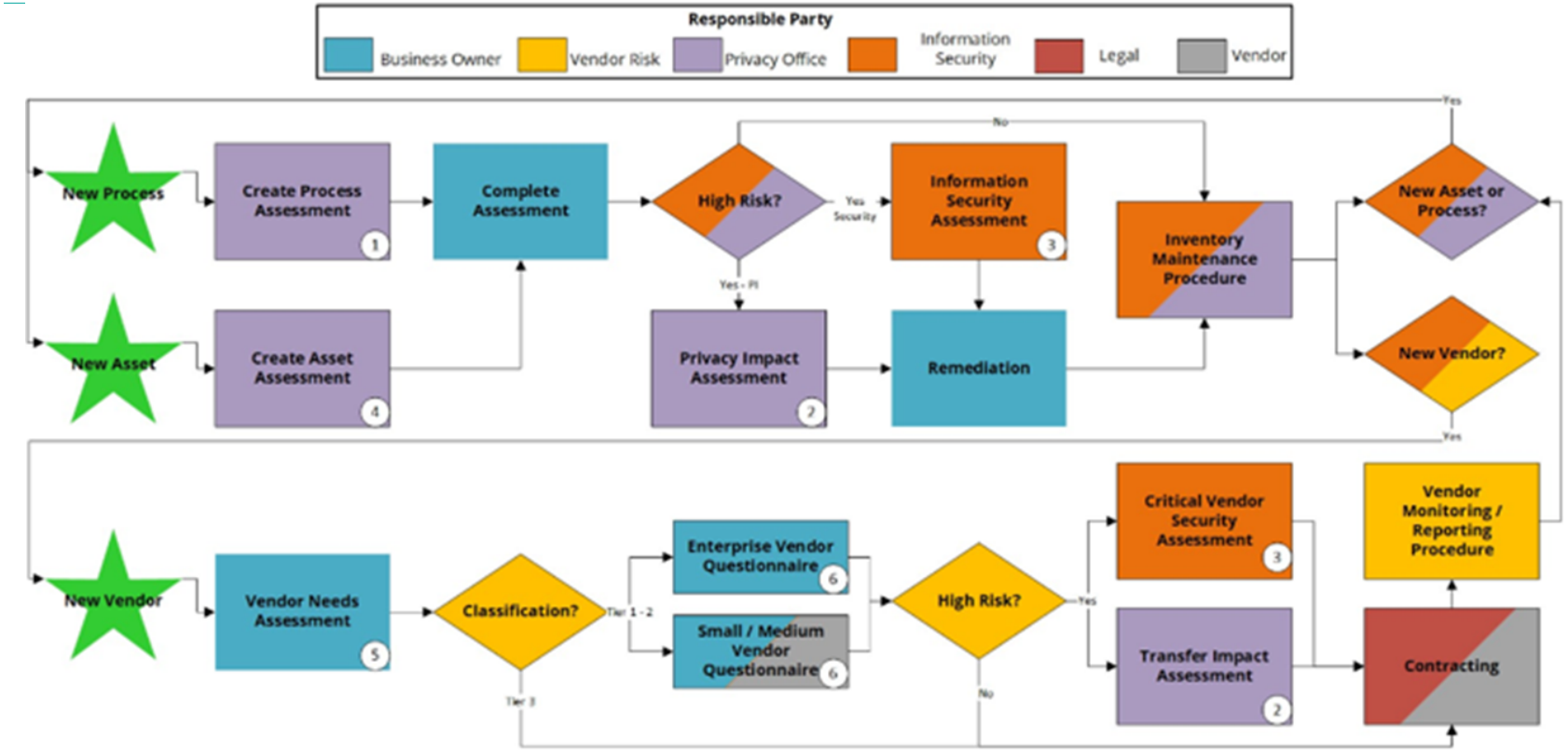
Operationalizing Impact Assessments

Operationalize it internally….



Assessment Workflow

SQUIRE PATTON BOGGS



SQUIRE PATTON BOGGS

OK, so what does an assessment look like?

Basic to Vendor Assisted

ICO's Template

https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf

SQUIRE PATTON BOGGS

1. Identify need for assessment
2. Describe the processing
3. Meet with stakeholders
4. Necessity and proportionality
5. Identify and assess risk
6. Measures to reduce risk
7. Signoffs and outcomes

ICO Sample: Word or Excel…or….

SQUIRE PATTON BOGGS

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

SPB's Shortcut to Compliance

SQUIRE PATTON BOGGS

SPB Developed 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)
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)
5. Guidance on developing and maintaining an information governance program (SPB clients)
6. Template company policy on conducting assessments (SPB clients)

Developing Impact Assessments with Third Party Tools

SQUIRE PATTON BOGGS

Benefits Include:

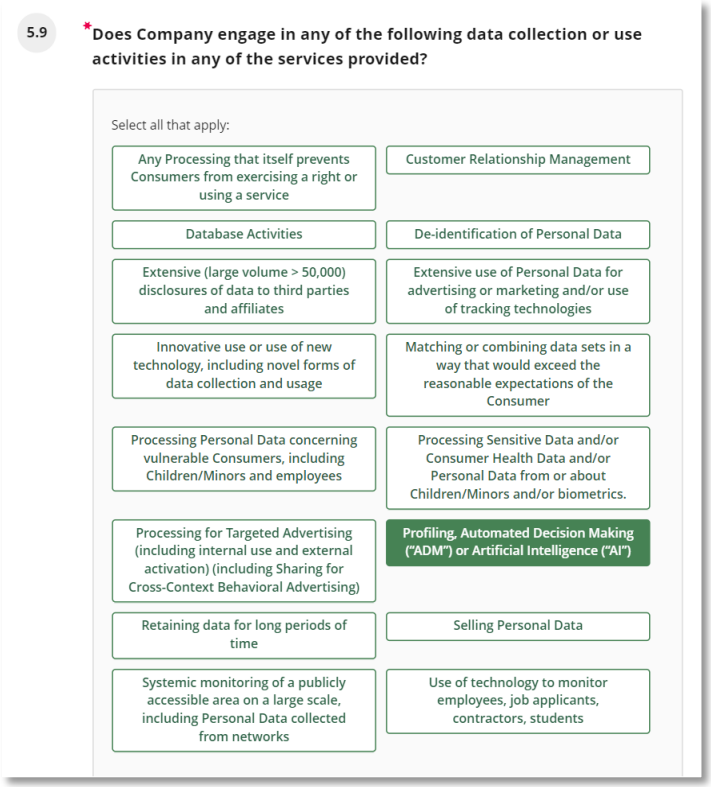
1. Customized, user-friendly assessments
2. Use of conditional logic which shows or hides questions, sections, or content based on how respondents answer previous questions
3. Customized rules to auto launch additional assessments based on respondents' answers
4. Collaboration between business owners 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

SPB's Impact Assessments in OneTrust

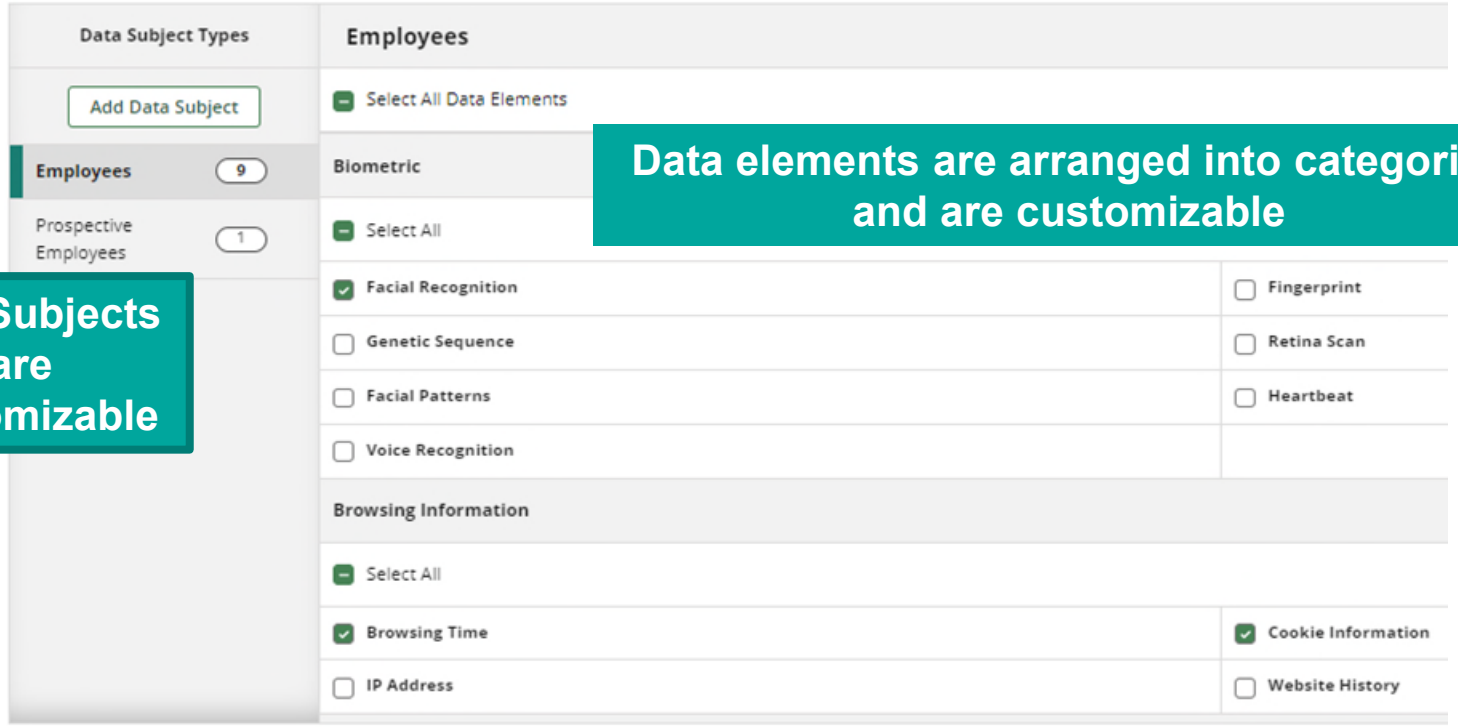
SQUIRE PATTON BOGGS

Use Rules to Launch New Assessments

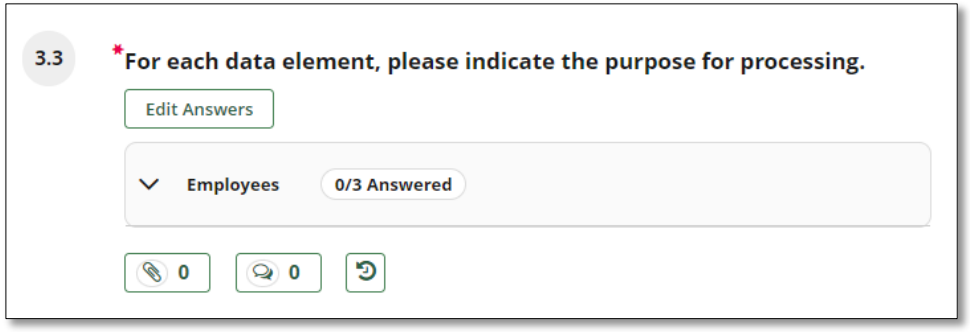
We can use rules to launch additional questionnaires, depending on how the respondent answers questions. In this case, we can launch separate assessments if an activity is selected that requires additional controls, such as Children / Minors Data, Health Data or Artificial Intelligence.

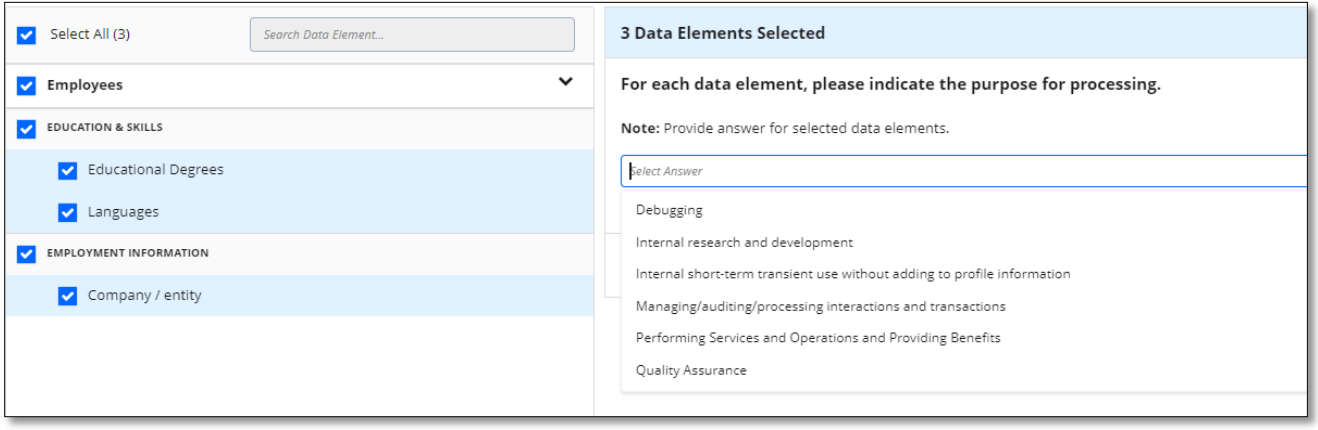


Impact Assessments



Impact Assessments





Key Takeaways

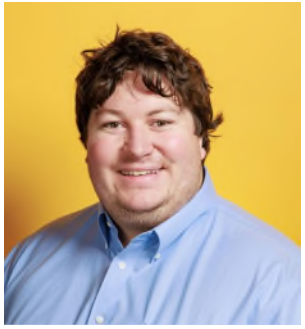
SQUIRE PATTON BOGGS

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

Contacts

SQUIRE PATTON BOGGS

Kyle R. Dull
Senior Associate
Squire Patton Boggs (US) LLP
Kyle.Dull@squirepb.com



Daniel McVay
CIPP/US/C, CIPM, AIGP
Corporate Counsel Product Privacy, LCPO
Intuit
Daniel_McVay@intuit.com

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

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