May 11, 2023

# PIA Bootcamp: Getting Your PIAs Compliant

Privacy+ Security Forum

# Speakers

**Erin Butler**
Lead Global Privacy and Cyber Risk Organization
Under Armour

**Liz Roberts**
Senior Privacy Counsel
DuckDuckGo

**Jennie Cunningham**
Associate
Kilpatrick Townsend & Stockton LLP

**Amanda M. Witt**
Partner
Kilpatrick Townsend & Stockton LLP

# Agenda

- Background
  - Applicable Laws
  - Jurisdictional Considerations
  - Terminology Refresher
- Designing the Process
- PIA Considerations
- Bootcamp Checklist
- Q&A

# Background: Applicable Laws

**Many jurisdictions require privacy impact assessments by law, and PIAs underpin requirements for any privacy/data protection law. Key jurisdictions include:**

- **EEA/EU/UK**
- U.S. states: **VA, CO, CT, IN, TN, MT,** [**CA** - tbd]
- Canada: **Quebec**
- APAC: **China, Japan,* Australia,*** Philippines, Vietnam, Singapore, South Korea
- LATAM: **Brazil, Argentina**, Colombia
- EMEA:, Israel, Kenya, Nigeria, South Africa
- AI assessments, e.g., NYC, EEA, US (NIST)

*not mandatory but strongly recommended

**Even where not technically "required" PIAs are the primary method used to:**

- Determine if a DPIA is required (e.g., under GDPR)
- Meet critical privacy by design, accountability, risk assessment, and security obligations under privacy law
- Follow established frameworks, such as NIST

# Jurisdictional Considerations: EU/EEA/UK

**Goal: Design PIA process/platform/assessment to account for jurisdiction-specific PIA requirements, while maintaining an overall manageable baseline**

- PIAs are critical in enabling companies to meet privacy by design, accountability, and transparency/notice obligations under GDPR; determining whether a **DPIA** is required
- **When is a DPIA required?**
- **What goes in a DPIA?**

# Jurisdictional Considerations: US States

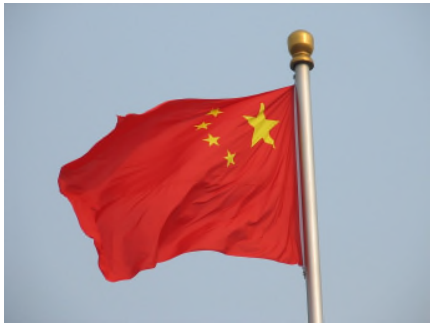
Privacy+ Security Forum

| State (effective date) | PIA required? |
|---|---|
| **Virginia (Jan. 1, 2023)** | Yes |
| **Colorado (July 1, 2023)** | Yes; regulations detail |
| **Connecticut (July 1, 2023)** | Yes |
| **California (CPRA Jan. 1, 2023)** | regulations are expected on when to submit a "risk assessment" to the California Privacy Protection Agency |
| **Montana (Oct. 1, 2024)** | Yes |
| **Tennessee (July 1, 2025):** | Yes |
| **Indiana (Jan. 1, 2026):** | Yes |
| **Utah (Dec. 31, 2023** | No |
| **Iowa (Jan. 1, 2025)** | No |

- PIAs must be disclosed to the attorney general, if requested.
- **When is a DPA required?**
- **What goes in a DPA?**

# Jurisdictional Considerations: Canada and China

- **Canada:**
  - **Federal:** No current requirement/recommendation for private sector entities under PIPEDA. Bill C-27 would require a PIA.
  - **Quebec**: Bill 64 requires companies to conduct a PIA, including where personal data is transferred and stored outside Quebec, effective September 2023.
- **China:** DPIAs are required under PIPL Art. 55 in certain circumstances



# Jurisdictional Considerations: Other

- **Australia:** recommended
- **Argentina:** required in certain circumstances
- **Japan:** encouraged, but not mandatory under the APPI
- **Brazil**: The regulatory authority issued Q&A guidance in April 2023. PIAs recommended for:
  - large scale or significant impacts processing **PLUS**
  - sensitive personal data, new tech, surveillance, automated decision-making, and/or vulnerable populations
- **Other jurisdictions:** Colombia, Israel, Kenya, Nigeria, Philippines, Vietnam, Singapore, South Africa, South Korea

***Takeaway: While there are differences among jurisdictions that need to be considered, the core of the PIA will largely assess the same items across the regions.***

# Refresher: Terminology

Privacy+ Security Forum

**Privacy Impact Assessment (PIA):** an analysis of how personal data is handled:

- (i) compliance with legal requirements;
- (ii) risk and effects of collecting, maintaining, and using personal data, and
- (iii) evaluation of protections and alternative processes to mitigate potential privacy risks.
- Generally, a PIA should cover
  - **what** personal data is being collected,
  - **why** it is being collected/**intended uses**,
  - **whom** the personal data will be shared with, and
  - **how** the personal data will be maintained.

- **Data Protection Impact Assessment (DPIA)**: an assessment required (usually under GDPR) for certain high-risk personal data processing that conducts a risk-analysis that balances the benefits of a specific processing operation involving personal data against the potential for harm to data subjects.

# What activities would trigger a PIA?

Privacy+ Security Forum

At the fundamental level, any project involving the *processing* of personal information/personal data would be evaluated using a PIA, but it is important to recognize that certain activities should always trigger a PIA and warrant high priority for assessment.

- **The business units should receive training so that they:**
  - Recognize “personal information”
  - Recognize when to fill out the threshold questionnaire
  - Identify existing projects that need a PIA


**Sample “triggers” -- processing that involves:**

- Personal data originating in the EU/EEA.
- Personal data originating in jurisdictions such as China, CA, CO, VA, Quebec, Argentina, Brazil, etc.
- Profiling
- Sensitive data
- Minors’ personal data
- Large number of data subjects
- Targeting advertising/marketing
- Sales of personal data
- Transferring personal data from one country to another
- Third party access to personal data

# Who should be involved?

- A common issue is how to get the right people and teams linked into the PIA process.
- Training and awareness is key, but how do you first identify and loop in the teams that should be involved in PIAs?
- A mandate and executive support is important.
- What other processes should be linked to the PIA process?

**The process usually involves:**

| Who | What |
|---|---|
| Privacy Office | Maintain PIA forms and documentation, facilitate |
| Legal/Privacy Legal | Review/approve |
| Privacy Managers | Review/approve |
| Security/ITS | Provide input; approve sections |
| Vendor management/TPRM | Provide input; approve sections; coordinate/link to vendor assessments |
| Risk management | Role varies by organization |
| Business units | "Own" the project; primary responsibility for input and completing the PIA, answering questions, implementing remediation measures |

# Identifying likely PIA “candidates”

- **Marketing**: The marketing department is always looking to take advantage of the latest and greatest in ad tech, targeted advertising, profiling, customer 360, omnichannel, and similar technology. Many of these initiatives will require a PIA, especially those that involve, for example, profiling of customers.

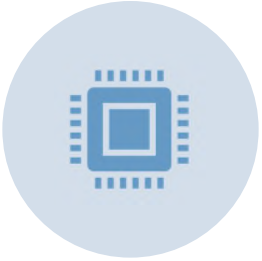
- **Product developers**: Development teams frequently seek to use personal data in designing new products, projects, software. Often, certain initiatives can be mitigated in terms of limiting the use of personal data or using techniques like pseudonymization, and PIAs will allow much greater visibility into these areas of the business. For example, designing products like “virtual try-ons” potentially carries risk related to the processing of biometric data.

# Identifying likely PIA “candidates”

**HR**: The nature of HR entails routine processing of personal data, and there may be risk around the use of vendors, onboarding and offboarding procedures, and especially around the handling of **sensitive/special categories** of personal data, e.g., health information.

**CRM**: Depending on the nature of the CRM function, representatives frequently work with customers and handle personal data. CRM may have an automated aspect and numerous vendors are often involved. Automation using, for example, **AI or voice recognition** should be evaluated.

**Analytics**: Often tied to profiling, advertising, and/or marketing, conducting analytics on personal data is frequently an area of personal data overuse, unauthorized secondary use, and oversharing among departments, with vendors.



**Manufacturing sites**: Tied to HR, factories and similar sites may collect personal data, with functions such as biometric logins or timeclocks that should be evaluated.

# Vendor or DIY?


- **Question:** Build and maintain a PIA process from scratch/manually or to invest in a vendor platform?
- Depends on factors such as:
  - Privacy program maturity
  - Resources
  - Budget
  - Volume of PIAs (current and anticipated)
  - Processing activities
  - Applicable law
  - Value-add of the vendor platform

# Designing the template


**Consider:**

- Baseline requirements/must-haves
- Business-specific questions
- Threshold questionnaire / conditional logic
- Full PIA / conditional logic
- DPIA / conditional logic
- Linking to other processes and assessments
- Identifying owners, reviewers and approvers
- Format, tool, platform, vendor

# Designing the template

Privacy+ Security Forum

**So you have a PIA process…how do you get this thing off the ground?**

- **Documentation**
  - Clear, concise procedures
  - Links to the PIA in relevant policies/assessments
- **Awareness campaign**
  - Who do we need to reach?
  - What kind of messaging is involved?
  - What are the delivery methods?
  - What's likely to be effective and will this differ by group?
- **Training**
  - In addition to the above, who will design the training and what will it look like?
  - Who will be responsible for delivering the training?

# Where are the risks and do we manage them?

Privacy+ Security Forum

- Trend of CISOs getting targeted in data breaches
- Risk register; risk of documenting risk…
- EU, US and other regulators are going to look for the PIA documentation
  - Consultation obligation – when to talk to the regulator
  - US cyber insurance

# “But do we NEED a PIA?”

## PIAs as best practice and why

- Documentation
- Privacy program fundamental – accountability, oversight
- Supports most other privacy obligations
  - Data mapping/ROPA
  - Privacy notices
  - Third party management
  - DPIAs
- Understand what’s happening at the organization with personal data, products/services in development
- Identifying risks and potential issues
- Staying ahead of the game

# Oversight and Follow-up

## We did a PIA….can we relax now?

- Check the box vs. ongoing obligations
- What happens after you click “Approve”
- Conditional approvals

- PIA approval may be made conditional upon the business implementing certain measures. **Sample remediation measures include:**
  - data minimization
  - update privacy policy/notice to account for new type of processing (transparency)
  - new consent mechanism
  - additional security measures (physical, technical, organizational)
  - anonymization / pseudonymization
  - appoint/assign person responsible for oversight
  - attestations
  - enter into data protection agreement with third party
  - conduct additional assessments – e.g., vendor risk assessment, transfer impact assessment

# Other issues and stumbling blocks

Privacy+ Security Forum

- Budget/resources
- Enforcement and overall buy-in
- Oversight and ongoing monitoring
  - Projects that change scope (e.g., U.S. app launches in Europe or Japan)
- Adapting the PIA to ever-changing laws and developments (e.g., generative AI)
- What other issues have you encountered?

# Bootcamp checklist

Privacy+ Security Forum

- ❑ Identify applicable laws - set baseline and identify heightened requirements
- ❑ Design overall process flow and begin to fill in details - it does not have to be perfect and it will change!
- ❑ Identify PIA triggers - required by law and activities particular to the business
- ❑ Identify roles and responsibilities and plug them into the process
- ❑ Identify likely PIA candidates within the business and prioritize those for launch/focus
- ❑ Consider DIY, vendor, or hybrid
- ❑ Identify budget and resources
- ❑ Adjust the process as needed
- ❑ Design training and awareness (try to do awareness as you go); prepare for challenges from the business
- ❑ Identify PIA risks
- ❑ Launch! Reassess after pilot period

# Q&A

Privacy+ Security Forum