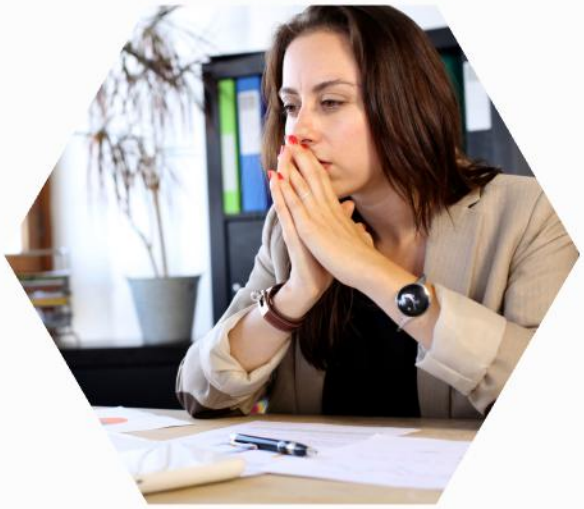
THE PRIVACY PRO

HOW WE HELP

PRIVACY IMPACT ASSESSMENTS

We equip you with the tools, skills, and mindset to implement a Privacy Impact Assessment program that works for business *and* privacy.

SOUND FAMILIAR, PRIVACY TEAM?



We spent all this money on privacy software that was supposed to do PIAs, data inventories, and DSARs.

It still doesn't work, but in the meantime we have a growing backlog of PIAs. The business isn't going to stop and wait for us!

We always learn about PIAs at the last possible minute, often after the project has gone live.

I don't know what isn't clear about the process. The business is supposed to engage us at the very beginning!

We simplified the assessment process! Now when we get a new vendor they complete a single form for privacy, security, AI governance, and procurement.

I think they also complete it for projects that don't involve a new vendor...right?

BUSINESS TEAMS ARE EQUALLY FRUSTRATED

I don't tell the Privacy Team how to do their jobs, why are they telling me I can't do mine?

I have a job to do and it requires data. I'm not trying to do anything shady, I just want to hit my targets and get my bonus.

The Privacy Team takes weeks to review the PIAs and then they come back with a list of problems for us to fix.

We're not trying to be difficult, we're just busy with a million other things. If they would tell us what to do, we would!

The policy says I have to fill out a form if my project includes "Personal Information". It doesn't! Just employee email addresses to login to the system. This is a waste of time.

© 2024 The Privacy Pro, Inc. All Rights Reserved

BE A BETTER PRIVACY PRO

Our jobs are complex, and it can feel like we're carrying the weight of the world. Privacy teams are often under-resourced, with responsibilities and risks constantly growing.

PIAs may feel like just another item on your to-do list, but they're actually a tool to help manage your ever-expanding mandate.

Reduce friction

Privacy is complicated, but it doesn't have to be hard—and it can even be fun.

Prioritize what matters

Focus on what's important. Let processes adapt as risks and priorities shift.

Give better advice

Make it your goal to never say "it depends" again.

BE A BETTER BUSINESS PARTNER

The PIA is an opportunity to be a true business partner. Being a good business partner means working together to get to 'yes' quickly and responsibly — supporting teams in using data to create innovative products and bring them to market.

Like any effective partnership, it relies on respect and clear communication.

Value people's time

As better questions, not more. Our PIA only has 15 questions, and none of them are about privacy.

Prevent surprises

Tell people what to expect so they can plan accordingly.

Get to the point!

Tell people what you want and why, be specific and action-oriented.

© 2024 The Privacy Pro, Inc. All Rights Reserved

THE PRIVACY PRO PHILOSOPHY

Our philosophy is straightforward: business goals should shape privacy requirements — not the other way around. While privacy professionals have long argued that privacy is a business imperative, the typical design of Privacy Impact Assessments (PIAs) doesn't reflect this belief.

In many cases, PIAs are over-engineered, attempting to eliminate human judgment and subjectivity from the process. With each new privacy law, PIAs tend to grow in length and complexity, and the original intent — to genuinely assess and address privacy risks — gets lost. Over time, completing the PIA becomes a task to check off, rather than a meaningful step towards managing privacy.

Ultimately, accountability lies with people, not processes or technology. This makes open conversations the most valuable part of any privacy assessment. A PIA shouldn't replace these conversations; it should document them.

A well-designed PIA is a record of the process by which we work together to:

- Understand the business context
- Document data practices
- Identify privacy risks
- Implement controls and safeguards

THE PRIVACY PRO APPROACH TO PIAS

TOOLS

- PIA Template in MS Excel format (can be customized for the organization or used as-is)
- Easy and accessible: only 15 questions for the business to answer
- Guidance and workflow built in using conditional logic (no macros or code)

PROCESS

- KEEP IT SIMPLE! Share it via email, use a shared drive, print it, fax it—just get started!
- Self-serve model for lower risk initiatives
- PIA is an artifact of conversations; it does not replace them

PRIVACY OUTCOMES

- Documented understanding of data in its business context
- Confidence that the business has the tools, clarity, and incentives to manage privacy responsibly
- Ability to demonstrate accountability

BUSINESS OUTCOMES

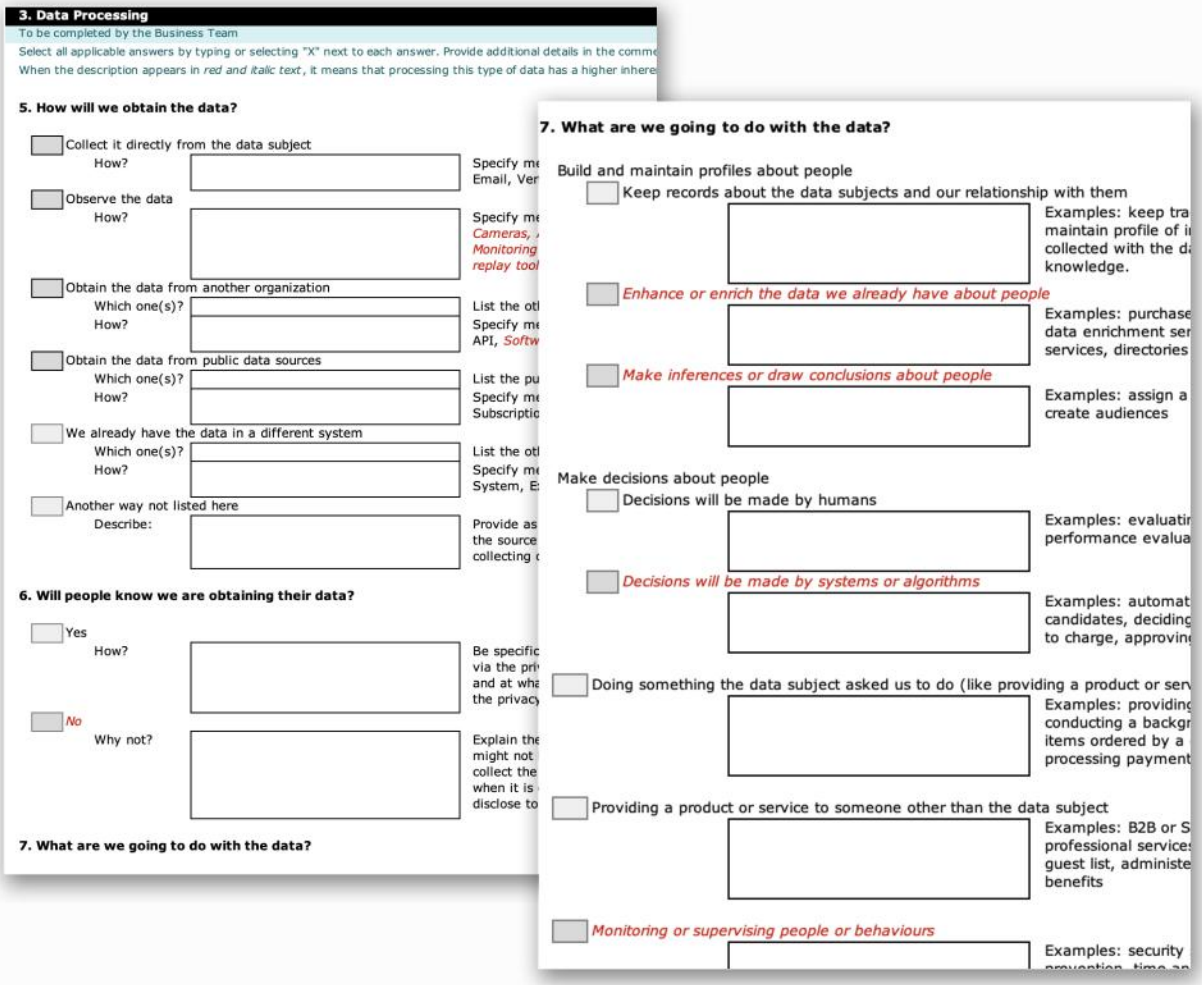
- Actionable steps with a clear definition of 'done' for each task
- Insight into *why* a requirement applies (not just 'applicable law')
- Information needed to make decisions and accept risk

© 2024 The Privacy Pro, Inc. All Rights Reserved

15 QUESTIONS FOR THE BUSINESS

It took over 15 years to narrow down the 15 questions that truly matter. Surprisingly, that wasn't the hardest part—the real challenge was making them multiple-choice! The questions are guided by three key principles:

- **Relevant:** Ask only questions where the answer directly affects privacy requirements. The PIA isn't a substitute for a data inventory or ROPA.
- **Focused:** Frame questions so they can be answered without needing to login or look anything up. We perfected this approach with a client whose team would only participate via phone during their commute!
- **Objective:** Avoid subjective terms (like necessary, adequate, reasonable) and defined terms (like anonymous or personal information).



3. Data Processing

To be completed by the Business Team

Select all applicable answers by typing or selecting "X" next to each answer. Provide additional details in the comme

When the description appears in *red and italic text*, it means that processing this type of data has a higher inhere

5. How will we obtain the data?

☐ Collect it directly from the data subject
How?

☐ Observe the data
How?

☐ Obtain the data from another organization
Which one(s)?
How?

☐ Obtain the data from public data sources
Which one(s)?
How?

☐ We already have the data in a different system
Which one(s)?
How?

☐ Another way not listed here
Describe:

6. Will people know we are obtaining their data?

☐ Yes
How?

☐ *No*
Why not?

7. What are we going to do with the data?

7. What are we going to do with the data?

Build and maintain profiles about people

☐ Keep records about the data subjects and our relationship with them
Examples: keep tra maintain profile of i collected with the d knowledge.

☐ *Enhance or enrich the data we already have about people*
Examples: purchase data enrichment ser services, directories

☐ *Make inferences or draw conclusions about people*
Examples: assign a create audiences

Make decisions about people

☐ Decisions will be made by humans
Examples: evaluatir performance evalua

☐ *Decisions will be made by systems or algorithms*
Examples: automat candidates, decidinc to charge, approvin

☐ Doing something the data subject asked us to do (like providing a product or serv
Examples: providinc conducting a backgr items ordered by a processing payment

☐ Providing a product or service to someone other than the data subject
Examples: B2B or S professional service guest list, administe benefits

☐ *Monitoring or supervising people or behaviours*
Examples: security

RISK ASSESSMENT

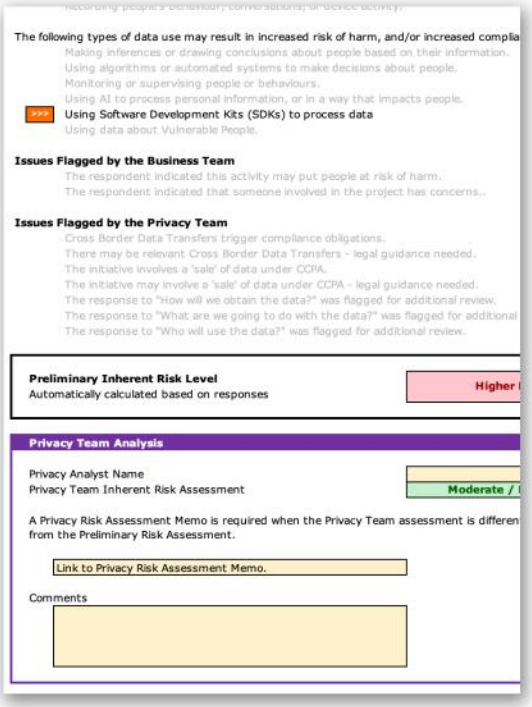
Conditional logic built into the spreadsheet calculates the Preliminary Inherent Risk Level (the risk that exists before any controls or mitigations are applied).

The preliminary inherent risk is based on responses to the 15 questions indicating:

- Higher-risk data types
  - Examples: biometric data, location data
- Higher-risk data processing
  - Examples: enhancing or enriching data by combining data sources, using SDKs to process data
- Issues flagged by the business team
  - Examples: the activity may put someone at risk of harm, someone involved in the project has concerns
- Issues flagged by the privacy team
  - Example: cross-border data transfers trigger compliance obligations, sale of data under CCPA

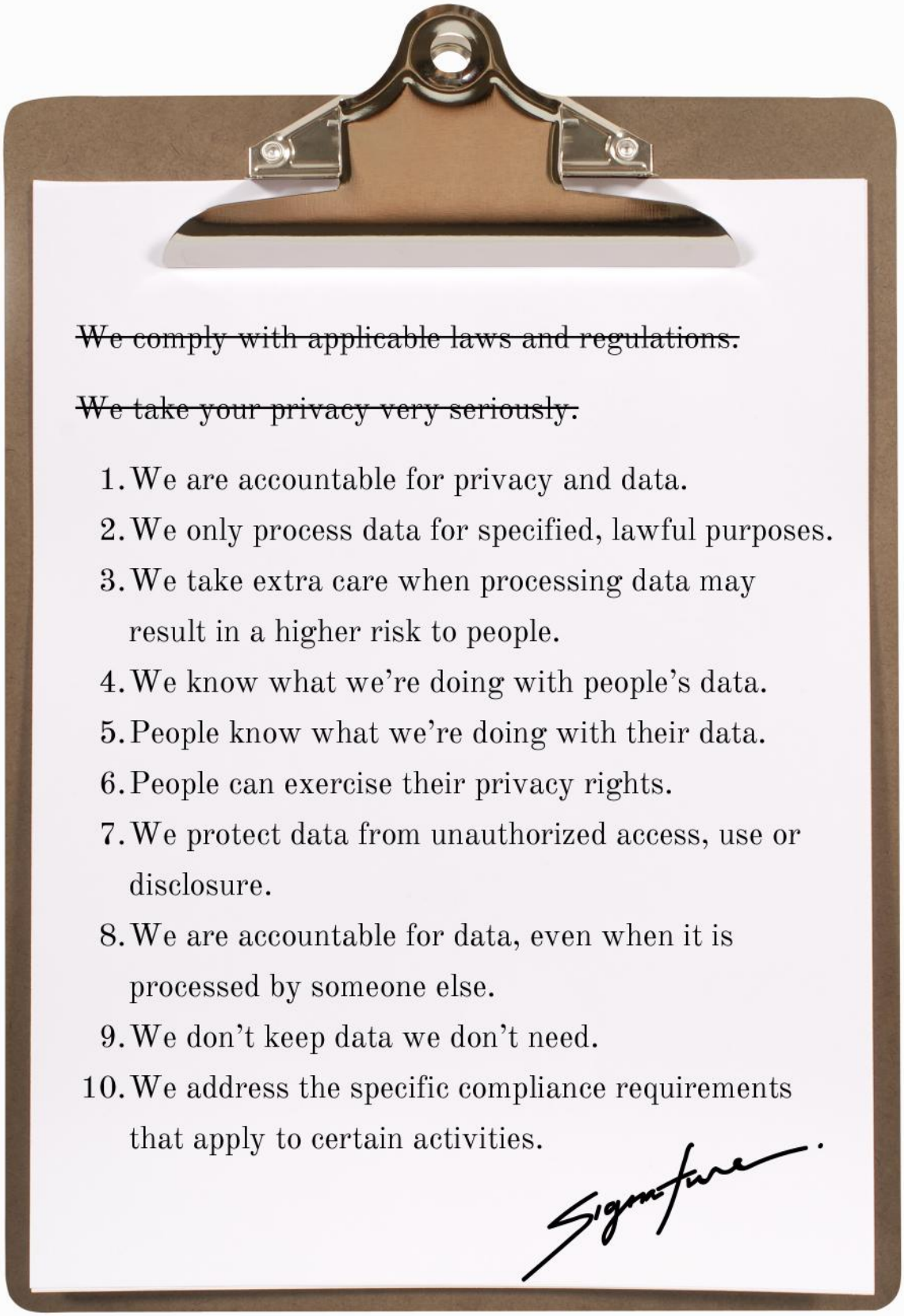
When the preliminary inherent risk assessment is moderate or low, the business team proceeds to implement requirements. The privacy team is available to help upon request.

When the preliminary inherent risk assessment is high, the privacy team reviews the PIA and provides guidance and guardrails. They may choose to override the preliminary assessment based on additional context.



© 2024 The Privacy Pro, Inc. All Rights Reserved

ACCOUNTABILITY STATEMENTS



~~We comply with applicable laws and regulations.~~

~~We take your privacy very seriously.~~

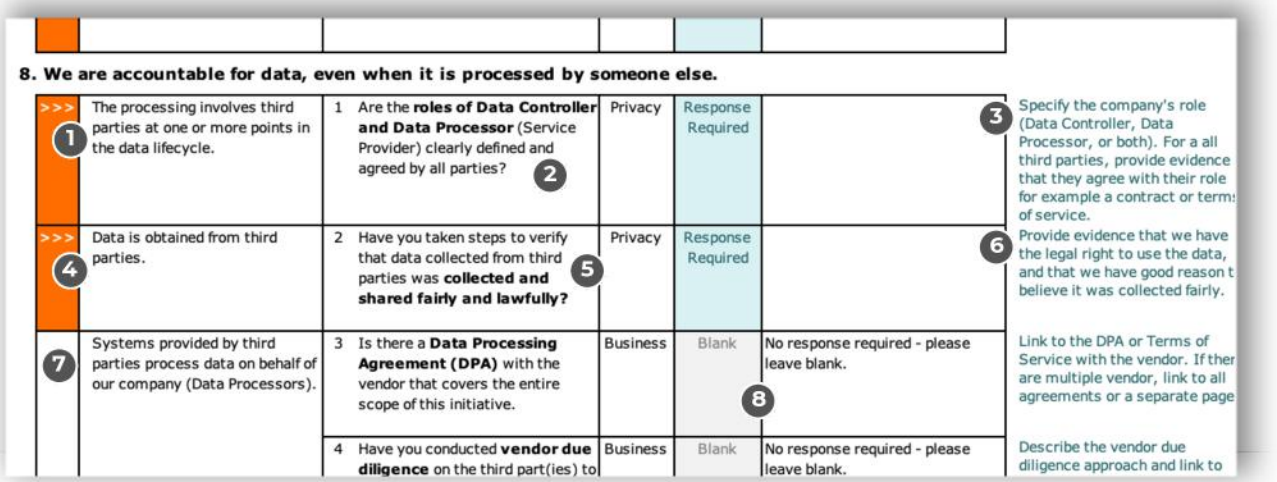
1. We are accountable for privacy and data.
2. We only process data for specified, lawful purposes.
3. We take extra care when processing data may result in a higher risk to people.
4. We know what we're doing with people's data.
5. People know what we're doing with their data.
6. People can exercise their privacy rights.
7. We protect data from unauthorized access, use or disclosure.
8. We are accountable for data, even when it is processed by someone else.
9. We don't keep data we don't need.
10. We address the specific compliance requirements that apply to certain activities.

Signature

PRIVACY REQUIREMENTS

A PIA should tell a story about the people whose data you are processing, why and how you use it, and how you protect it. The Privacy Requirements tab tells that story. It also spells out exactly what is expected and why.

To confidently make Accountability Statement #8. We are accountable for data, even when it is processed by someone else, we must be able to demonstrate, with evidence, that the answer to all applicable questions is 'yes'.



8. We are accountable for data, even when it is processed by someone else.						
>>> 1	The processing involves third parties at one or more points in the data lifecycle.	1 Are the **roles of Data Controller and Data Processor** (Service Provider) clearly defined and agreed by all parties? 2	Privacy	Response Required	3	Specify the company's role (Data Controller, Data Processor, or both). For a all third parties, provide evidence that they agree with their role for example a contract or term of service.
>>> 4	Data is obtained from third parties.	2 Have you taken steps to verify that data collected from third parties was **collected and shared fairly and lawfully?** 5	Privacy	Response Required	6	Provide evidence that we have the legal right to use the data, and that we have good reason t believe it was collected fairly.
7	Systems provided by third parties process data on behalf of our company (Data Processors).	3 Is there a **Data Processing Agreement (DPA)** with the vendor that covers the entire scope of this initiative.	Business	Blank 8	No response required - please leave blank.	Link to the DPA or Terms of Service with the vendor. If ther are multiple vendor, link to all agreements or a separate page
		4 Have you conducted **vendor due diligence** on the third part(ies) to	Business	Blank	No response required - please leave blank.	Describe the vendor due diligence approach and link to

(**1**) This initiative involves third parties, so (**2**) we need evidence to demonstrate that the roles of Data Controller and Data Processor are clearly defined and agreed upon by all parties. (**3**) You must indicate the roles and provide evidence that all parties are aligned, for example, with a contract or terms of service.

Because (**4**) we are obtaining data from third parties, (**5**) we must take steps to verify that the data was collected and shared fairly and lawfully. (**6**) Provide evidence of the steps taken and explain why we believe we have a legal right to use the data and that the third party collected and shared it fairly.

(**7**) The initiative does not involve third-party data processors, so (**8**) no response is required for this question.

© 2024 The Privacy Pro, Inc. All Rights Reserved

HANDS-ON PIA WORKSHOP

Our popular Hands-on PIA Workshop, tailored for your team.

We will meet with you to understand your goals (kickstarting a new PIA process, improving the existing one, raising awareness) and preferred format (length of time, number of participants). Workshops typically last 3-4 hours depending on your preference. This is a great way to help your team achieve their CPE targets.

The workshop covers:

- What is a PIA, and when should it be completed?
- Differences between PIAs in the public, health, and private sectors
- Common mistakes when completing a PIA
- How to complete a PIA via a hands-on case study exercise in class

You also get:

- Access to The Privacy Pro's methodology and PIA template, minor modifications included.
- An example completed PIA with our recommended solution to the case study (select a pre-made case study or we can create one specifically for you for an additional fee).
- Certificate of completion
- Continuing Privacy Education (CPE) credits
- A digital badge to add to your LinkedIn profile

I am incredibly thankful to have participated in the Privacy Impact Assessment Workshop hosted by The Privacy Pro Academy. The insights gained were invaluable, and the collaborative environment made the experience even more enriching. A special shout out to Nick for creating a safe and engaging space to learn, share and discuss all things related to PIAs.

PIA PROCESS IMPLEMENTATION

Everything you need to kick-start your PIA program

PIA Procedure and Workflow

- Documented procedure for intake, data collection, triage and escalation, and requirements implementation
- Roles and responsibilities for PIAs
- Job aid: When is a PIA required?

Bespoke PIA Template

- Customized PIA template, branded with your logo and colors.
- License to modify and use the PIA Template for internal purposes.

Virtual PIA training for business teams

- Why do PIAs, when to do them, your responsibilities (not a spreadsheet tutorial or step-by-step)
- Slide deck provided and meeting recorded

Initial PIA Support for the privacy team

- Up to 3 hours of consulting support for the initial PIA, which may include attending meetings, reviewing documents, and answering questions.

Thank you to Nick, Lauren, and The Privacy Pro for a practical approach to PIAs! They provided clear context and tips to ensure participants don't let PIAs become a "tick the box" exercise.

In fact, they gave pathways to enable business teams and privacy teams to partner on reducing risk together - and even help reduce timelines to complete PIAs. And in comparison to the jargon-heavy legalese templates from many regulators and law firms, The Privacy Pro template is easily accessible for folks who don't speak privacy-specific jargon.

© 2024 The Privacy Pro, Inc. All Rights Reserved

HOW THE PRIVACY PRO HELPS

Extended PIA support

We are always happy to provide additional support while you operationalize the PIA process.

- Expert guidance on handling complex, layered PIAs. We can do this on an ad-hoc basis or a monthly retainer to keep it predictable.
- Coaching for privacy teams to build essential communication and project management skills.
- Customized action plans to address PIA backlogs with a risk-based, business-aligned approach.

Extra set of eyes

Our experienced consultants offer an objective, expert perspective to strengthen privacy practices and identify areas for improvement.

- Spot potential blind spots and areas for enhancement.
- Offer constructive, non-legal feedback on privacy assessments and decisions.
- Share insights on industry trends and best practices in handling PIAs and privacy challenges.

HOW THE PRIVACY PRO HELPS

PIA Business Partner

Embedded within your business team, we help streamline PIAs, making it easier for privacy teams to say “Yes, and…” to business initiatives.

- Anticipate and address privacy issues proactively within the business team.
- Champion business goals while aligning with privacy requirements.
- Provide detailed context to privacy teams for more efficient reviews.

General Privacy Support

We help companies develop, mature, and optimize privacy programs that are aligned with business goals and regulatory requirements.

- Design and monitor privacy metrics with clear, actionable reporting.
- Establish privacy risk guardrails to guide decision-making.
- Map data processing activities to articlulate data use and data flows in context.

© 2024 The Privacy Pro, Inc. All Rights Reserved

ABOUT THE PRIVACY PRO

The Privacy Pro is a boutique privacy consultancy that helps organizations shift the mindset that privacy is a roadblock, enabling them to leverage data to achieve business goals without compromising on privacy.

We are known for our pragmatic approach, focusing on getting the job done without scaremongering or over-complicating matters. With global experience across various industries, we provide practical and efficient solutions, using templates, tools, and past examples to accelerate projects.

We established The Privacy Pro Academy to equip the industry with privacy professionals with the skills organizations need. We are building an inclusive and responsive community of excellence in privacy education. We aim to make privacy a profession chosen by people committed to social justice and driven by purpose to respect people and their data.

Lauren Reid

CEO & Founder
The Privacy Pro

she/her

Nicholas Cheung

Executive Director
The Privacy Pro Academy

he/him

OUR VALUES

Respect

We value everyone and treat people with dignity and professionalism.

We honour each other's time, boundaries, and ideas.

We have a strict 'no assholes' policy.

Integrity

We build trust through responsible actions and honest relationships.

We admit when we make mistakes, and when we don't know the answer.

We don't sell services that clients don't need.

Inclusion

We bring our whole selves to work: our flaws, quirks, passions, humour, and vulnerability.

We value what you can do over what you have done.

We work to improve the diversity, equity, and inclusiveness of our team and the privacy profession overall.

Collaboration

We treat others as colleagues, not competition.

We believe there is plenty of success to go around, and that relationships are more important than revenue.

Community

We use our privilege to meaningfully support causes we believe in without being performative.

We make time for pro-bono work, mentorship, and advocacy.

© 2024 The Privacy Pro, Inc. All Rights Reserved