Making privacy core business

What makes a great Privacy Impact Assessment?

Updated March 2024

First published March 2021

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 1, 60 Martin Place, Sydney NSW 2000, Australia

Table of Contents

1. Executive summary

1.1 Overview

Whilst privacy risks are becoming key risks for most organisations, there is little information to guide the business or government decision maker on what makes a great privacy impact assessment (PIA). This article explains to decision makers what a PIA is and what it is not, what to consider when making decisions about the need to conduct a PIA, when and why a PIA should be done, what a PIA should cover, who should do it, what to look for in a skilled PIA provider and whether (once completed), the PIA should be published.

1.2 The "Essential Eight" for a great PIA

The "Essential Eight" guides public and private sector organisations on the essential cyber security mitigation strategies that organisations should have in place for baseline security. Whilst the Essential Eight are pitched as baseline security, the reality is that many government agencies and private sector entities do not have them all in place.

This paper adapts the concept of an "essential eight" and has applied it to the key criteria that contribute to a great PIA, as summarised below.

Privcore's "Essential Eight" for a great PIA	
1) ADDRESS HIGH RISKS	Performed for high risk personal information processing activities
2) ONGOING	Initiated at the right points of the project's life (early development, prior to launch, regular intervals after launch)
3) BUY-IN	Has buy-in from business and/or government decision makers
4) WELL-DEFINED SCOPE	Ensures a holistic lens can be applied through a well-defined scope
5) ADDS VALUE	Conducted from a performance perspective, not just compliance
6) DOWNSTREAM LENS	Looks at the risks not just of the organisation, but also its customers' or citizens' risks and potentially other participants in the ecosystem
7) RESOURCED	Resourced, as appropriate, internally or externally with a PIA provider that meets applicable criteria
8) AVAILABLE	Is available to the public – particularly where public trust and confidence is valued

2. What is a PIA?

A PIA is a risk assessment of new or existing processes, technology, laws or regulations, systems or programs for example (hereinafter referred to as projects) involving personal information. It is designed to identify the privacy risks of handling the personal information in the project. It can also be used to draw out positive aspects of the project, such as greater security or minimal data collection. Once privacy risks are identified, recommendations can be made to manage, mitigate, prevent or eliminate identified privacy risks.

Most privacy or data protection regulators provide their own guidance about what a PIA is, which largely reflects the above. Some privacy regulators also produce specific guidance or examples of how to undertake PIAs. A handful of those guides and examples are linked to below:

Australia	Office of the Australian Information Commissioner
• NSW	Information and Privacy Commission
• Victoria	Office of the Victorian Information Commissioner
New Zealand	Office of the Privacy Commissioner
Singapore	Personal Data Protection Commission Singapore
Europe	European Data Protection Board (endorsement of WP29 Guidelines)
UK	Information Commissioner's Office
USA	Department of Justice
Canada	Office of the Privacy Commissioner of Canada

2.1 What is a PIA NOT?

As important as what is a PIA, is what it is not. A PIA is NOT:

A PIA is NOT:	Rather:
About outsourcing risk	It is about managing risk of the entity performing or requesting the PIA, AND impacted individuals such as customers. Too often PIAs are performed only from the perspective of the client's risk, and not from the perspective of individuals whose information the client handles.
A ticket to justify decisions already made	Sometimes a PIA is requested at the last minute when decisions to implement projects have already been made. Rather a PIA is an independent process which helps inform whether it is appropriate to continue the project in the way envisaged.
A purely compliance or legally driven checklist	A great PIA considers non-legal and compliance related risks as well, such as customer expectations, business operational risk, technology issues, community attitudes and relevant stakeholder views.
A marketing tool	The project's description is designed to facilitate an understanding of the project from a layperson's perspective.
Long and complex and full of legal or technical jargon	It uses plain language.
A one-time exercise	It is done at appropriate points in the project's lifecycle (design stage, prior to launch, post launch).

For more on what a PIA is NOT, see the Canadian and New Zealand privacy regulators.

3. When should you do a PIA?

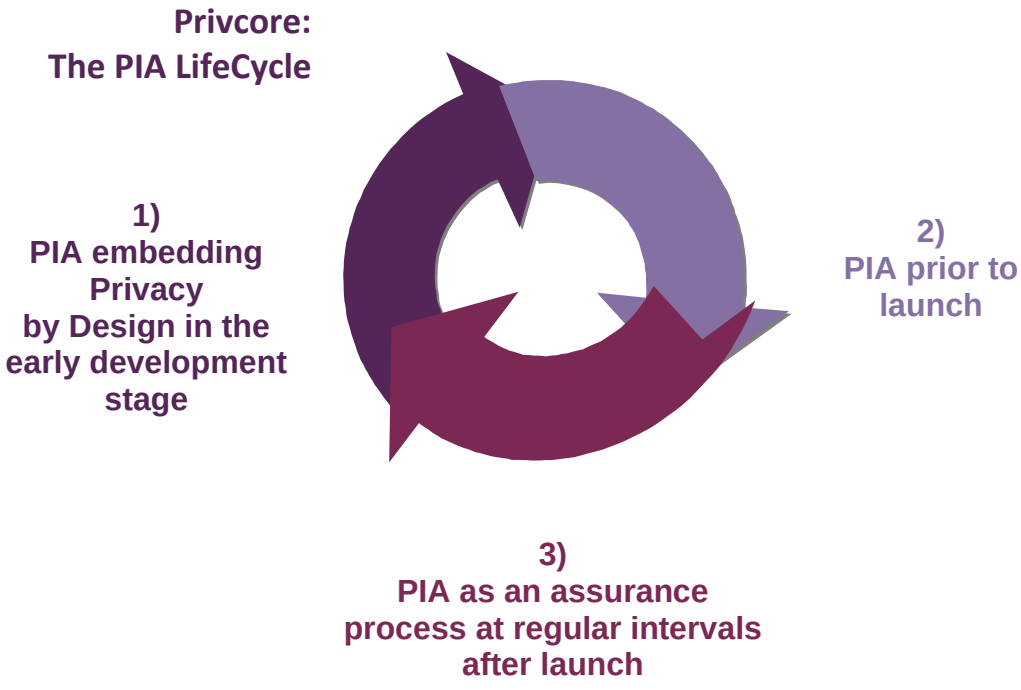
Existing enterprise risk management, procurement, or business processes should assist with the trigger to conduct a PIA. For example, when completing the business case or funding requests for a project, part of the approval process should include the consideration of a PIA, where that project involves the handling of personal information. This is particularly necessary where high risk processing activities are involved, including AI.

Recent changes to the Digital Restart Fund in NSW exemplify this type of approach. Prior to granting approval for funding from the Digital Restart Fund, digital projects must have privacy considerations taken into account, as enacted in section 10 of the *Digital Restart Fund Act 2020* (NSW). The NSW Information Privacy Commission's submission to the Inquiry into the provisions of the Digital Restart Fund Bill specifically emphasised that it expects "before agencies are granted funding for their Digital Restart projects, they explain how they will comply with [applicable privacy legislation]. This can be done by way of a PIA which identifies privacy risks of a program and how those risks can be mitigated. Privacy

compliance should be incorporated into the design of the project for which funding is sought from the Fund".

Further, in relation to projects involving AI, NSW government has developed an AI Assurance Framework which requires projects using AI funded through the Digital Restart Fund or which exceed a cost of $5 million to be submitted to NSW's AI Review Committee for review. This is in addition to any PIAs that should be undertaken. Only a small number of projects have been reviewed under the AI Assurance Framework, including FishOnline (NSW Fisheries), Natural Language Analysis of Submissions (Information and Privacy Commission) and systems within the Regional NSW portfolio (p.67 Automated Decision-Making in NSW, Research Report, March 2024.

In addition to having PIAs at design and pre-commencement stages of the project, ongoing privacy risks should be monitored. Privacy risks continuously change, hence, management of those risks needs to be considered with a lifecycle frame of reference. The risks that may have been identified prior to the start of a project may have shifted dramatically once the project is operationalised and deployed. As such, PIAs need to be considered at multiple stages as shown in the following diagram:



Some privacy and data protection laws mandate when PIAs must be performed, whilst other jurisdictions consider PIAs good or best practice.

In Australia, since 1 July 2018, PIAs have been mandated for Federal government agencies for all "high privacy risk" projects under the Privacy (Australian Government Agencies - Governance) APP Code. These are projects that involve new or changed ways of handling

personal information that are likely to have a significant impact on the privacy of individuals (section 12 of the Code).

The OAIC has produced a threshold template that guides agencies with the appropriate questions to ask to determine if a project has “high privacy risk”. This includes the:

- amount and sensitivity of the personal information,
- nature of the cohort subject to the processing,
- level of impact on the relevant individuals,
- context in which the handling occurs, for example, whether it uses technology that is subject to negative discussion in the community; or
- level of control individuals will have over the way in which their personal information is handled.

Additionally, factors such as automated decision making, systemic monitoring or tracking, collecting information without the awareness of the individual and data matching or data linkage are red flags for the need to conduct a PIA.

The Australian Information and Privacy Commissioner may also direct agencies to undertake a PIA (s33D Privacy Act). PIAs, where not mandated, are regarded as good or best practice in New Zealand and in Australia for the private sector. It is expected as part of the reform of the Privacy Act in Australia that PIAs will become mandatory for the private sector as well, for activities with high privacy risks.

In the USA, PIAs are mandated for all federal government agencies that develop or procure new information technology that handles personal information (Section 208 of the E-Government Act). In the EU (and the UK post Brexit), PIAs (known as data protection impact assessments under the General Data Protection Regulation (GDPR)) are mandated particularly in the use of new technologies, where the nature, scope, context, and purpose of the handling of personal information is likely to result in a high risk to the rights and freedoms of people. Three specific categories are provided as examples in Article 35(3) of the GDPR, which has extra-territorial reach:

- automated processing of personal data that would produce legal effects or significantly affect people,
- processing large amounts of sensitive personal data, such as data revealing race, ethnic origin, political opinion, religion, genetics, biometrics, health, sexual orientation,
- systematically monitoring large public spaces

Under the GDPR the requirements to conduct PIAs apply equally to public and private sector organisations. Further, the recently adopted AI Act in the EU will also require fundamental rights impact assessments and conformity assessments in relation to high-risk AI systems. This would be in addition to any PIAs required under the GDPR.

3.1 Examples of high risk processing activities

- Dutch Ministry Covid-19 System – Processing contact tracing and covid testing records in the Netherlands with broad access by staff of information on millions of Dutch citizens as part of contact tracing and Covid testing, including their Citizen ID Number, date of birth and address with no logging of access, resulting in sale of personal information on the web and police investigations into staff alleged to have sold personal information.

- NSW mobile phone detection cameras – The world's first mobile phone detection camera program operating in NSW, designed to detect drivers using a mobile phone whilst driving using AI technology. A PIA was conducted but not released due to legal professional privilege. Some correspondence between the NSW Privacy Commissioner and Transport for NSW has been made available under a NSW Government Information (Public Access) Act request, though not included in public disclosure logs.

- Australian Bureau of Statistics (ABS) – Using linked data to investigate the role of sociodemographic factors in people with cancer in NSW – Adding data collected through the NSW Cancer Registry, BreastScreen NSW, NSW Pap Test Registry with data collected in 15 other data sets from the ABS, ATO, Department of Education, Skills and Employment, Department of Health, Department of Social Services and Services Australia. The ABS performed a PIA which the ABS engaged Privcore to review.

- The Robodebt scheme – a method of automated debt recovery that issued debt notices to welfare recipients with an automated data-matching system that compared Centrelink records with averaged income data from the Australian Taxation Office. Over a period of approximately four years it wrongly issued ~470,000 debts, which resulted in extensive media coverage and legal action with over $1.8 billion in repayments to citizens and other costs.

- The Dutch Tax Authority's anti-fraud scheme – used an automated risk classification model to find 'problematic' applications for child benefits, using a number of indicators including second nationality. The profiling resulted in thousands of families being wrongfully accused of fraud. The Dutch Parliament investigated and released a report in December 2020 titled "Unprecedented Injustice". As a result, in January 2021, the entire Cabinet of Prime Minister Mark Rutte resigned.

4. Why do a PIA?

Leaving aside the legal and compliance obligations that may require the conduct of a PIA, for example, in relation to high privacy risk activities, a PIA can be a helpful defence if something does go wrong and also help prevent problems in the first place. Quite often a PIA will have anticipated the potential risks and enables the organisation to head off problems that could otherwise arise when a PIA is not performed.

PIAs, especially when published, are also important tools to help build public trust and confidence in how the organisation handles customer and citizen personal information. A moderate investment upfront to identify and mitigate privacy risk can also save significant expense down the track.

The Office of the Victorian Information Commissioner has published an information sheet on 'Getting executive buy-in for privacy impact assessments', which further explains why PIAs are beneficial.

4.1 What should a PIA cover?

Determining the appropriate scope for the PIA is always critical. What is in or out of scope is often financially driven. The larger the scope the more time, resources and effort are required. Stakeholder engagement is a critical component of a PIA, but also very time consuming and thus impacts the budget allocated for the work.

Conducting a PIA from a performance perspective rather than a purely compliance perspective, ie: looking at the motivation, behaviour, performance and outcomes adds value to the PIA process and requires thinking beyond the minimum compliance requirements of privacy laws. This performance-based approach as opposed to a compliance-based approach, is commonly taken when regulating aviation safety.

For example, the Civil Aviation Authority describes the approach as follows: "we know that reacting after an incident or near miss is not the best way to prevent it happening again. We need to examine the causal factors more closely and transform our regulatory activities to follow a more risk and performance-based approach" (See: Ethical Business Practice and Regulation, Hodges & Steinholtz, 2017 p.67).

The same type of thinking is helpful when responding to a data breach and ensuring it does not recur or when there is a privacy incident that affects individual(s) in significant ways. An example of where a performance-based approach was not used was when Centrelink disclosed the claims history of one of its customers, Andie Fox, to the media in order to defend itself against alleged adverse claims. Whilst the Acting Privacy Commissioner at the time did not find there was an interference with the customer's privacy in the circumstances, the public backlash was strong.

The OAIC's Guide to Undertaking PIAs states at p.3 that "while PIAs assess a project's risk of non-compliance with privacy legislation and identify controls to mitigate the risk, a PIA is much more than a simple compliance check. It should 'tell the full story' of a project from a privacy perspective, going beyond compliance to also consider the broader privacy implications and risks, including whether the planned uses of personal information in the project will be acceptable to the community."

Most privacy regulators publish guides on what a PIA should cover, so, depending on your jurisdiction, this is always a good starting point.

5. Who should conduct the PIA?

If you've decided to do a PIA, you need to consider who should conduct it. The first consideration is whether staff within the organisation conduct the PIA or it is outsourced to an external PIA provider. There are advantages and disadvantages to each approach and the approach taken depends on a number of factors which can have various weightings within an organisation, including:

PRIVCORE – KEY FACTORS IMPACTING WHETHER A PIA SHOULD BE CONDUCTED INTERNALLY OR EXTERNALLY		
INTERNAL		**EXTERNAL**
Lower	Level of independence and objectivity sought	**Higher**
Lower	Level of public trust and confidence sought	**Higher**
Lower	Level of recourse required if something goes wrong	**Higher**
Lower	Extent of change to the way personal information will be handled	**Higher**
Lower	Level of internal biases	**Higher**
Lower	Funding available to conduct the PIA	**Higher**
Lower	Impact the project has on external stakeholders, particularly individual customers or citizens	**Higher**
Higher	PIA skills available internally	**Lower**
Higher	Whether the project has been the subject of a previous PIA	**Lower**

Based on the above table, the weighting towards outsourcing the conduct of the PIA to an external PIA provider can be greater, for example, where a high level of independence and objectivity is sought. In contrast, for example, where there are PIA skills available internally, the weighting towards conducting the PIA internally can be higher. All relevant criteria need to be considered as a whole to determine what may be most appropriate in the circumstances.

If the decision is made that an external PIA provider is needed there are generally three categories of PIA providers in the market:

- Privacy consultants or experts
- Law firms – lawyers will have varying levels of expertise in privacy

- Auditing companies – auditors will have varying levels of expertise in privacy

Law firms are commonly used when the client wants to claim legal professional privilege over the PIA – where they don't intend to release the PIA to the public. Whilst doing a PIA in these circumstances is better than not doing a PIA at all, it does not provide any opportunity to build public trust nor provide any transparency. Organisations could choose to publish their PIAs in part (for example where security information may be redacted). Often law firm provided PIAs are also compliance oriented only, and thus have a narrow lens and are less concerned about risks falling beyond the client.

Auditors tend to be used due to the pre-existing relationship they may have with the client due to audit work and are simply asked to add another lens to their audit work.

Privacy consultants or experts are increasingly being relied upon as the privacy profession matures and experts with the requisite skill enter the market. Some privacy consultants and experts have been in the market for more than twenty years. They commonly have privacy regulatory backgrounds and ensure that downstream risks (risks to individual customers or citizens are incorporated into the PIA). They may or may not have legal backgrounds too.

Alternatively, some clients decide to conduct the PIA themselves with an external review, which is an approach that works where there are staff internally with enough skill to be guided and who have expertise in the project. An example of this approach is ABS' PIA and review letter of 'Using linked data to investigate the role of sociodemographic factors in people with cancer in NSW'.

5.1 What to look for in a PIA provider

Look for providers that:

- Can put their feet into the shoes of their client's customers and thus understand risk from individual perspectives, as well as other stakeholders in the ecosystem
- Have staff with interdisciplinary skills – legal, technology, communications, business, regulatory experience
- Have critical thinkers on board
- Can enunciate both positive and negative privacy aspects
- Consider community expectations, impacted customers and citizens and other stakeholders
- Use plain language
- Charge fees in proportion to the quality and quantity of the work performed

Avoid:

- Those who take a tick box legal approach (as they generally do not meet privacy regulatory requirements and are limited to a purely compliance perspective)

- Those who only look at the interests of their clients and not the interests of their clients' customers or other stakeholders in the relevant ecosystem (as a PIA is designed to minimise risk to individual customers or citizens, not just the client's risks)

6. Should the PIA be published?

Publishing a PIA promotes organisational accountability and transparency. It also builds public trust and confidence. It takes courage to publish a PIA, because often PIAs will draw out criticism or negative aspects of the project. Responses to independent PIAs can be published to address any recommendations or perceived negative aspects. Components of PIAs that may be sensitive, such as security controls can always be redacted from the published version of the PIA. Sometimes summaries of PIAs are published.

Depending on which stage of the project's lifecycle the PIA is conducted may influence whether or not it is sensible to make the PIA publicly available. For example, PIAs conducted in very early stages of projects which may not proceed may lend themselves less to publication. However, PIAs performed prior to launch or as part of assurance processes may more readily lend themselves to publication.

The OAIC's APP Code for federal government agencies mandates the publication of a register of PIAs. It does not mandate publication of PIAs, themselves, but states they "may" be published. Some federal government agencies, like the ABS also publish the PIAs listed in their PIA register. Others like the Department of Health and Aged Care, the Australian Taxation Office, Services Australia and Attorneys-General's Department just maintain a register and list the PIA titles. Those interested to see a copy of a PIA need to submit an FOI request to obtain a copy. Sometimes even when they are released they are not published in the FOI disclosure logs in full or in part, and another FOI request needs to be made if another person wants a copy.

The OAIC's PIA register includes a summary of the subject matter of the PIA and also includes a list of threshold assessments it has undertaken. It does not include full copies of PIAs, therefore would also need to be requested through FOI.

7. Summary

A great PIA need not be a unicorn, but something we should increasingly see in the marketplace as the privacy profession matures and clients become more discerning. As a summary of the discussion in this paper, Privcore has developed the "Essential Eight" for a great PIA, adapting the concept of the "Essential Eight" from the cyber security space.

Privcore's "Essential Eight" for a great PIA	
1) ADDRESS HIGH RISKS	Performed for high risk personal information processing activities
2) ONGOING	Initiated at the right points of the project's life (early development, prior to launch, regular intervals after launch)
3) BUY-IN	Has buy-in from business and/or government decision makers
4) WELL-DEFINED SCOPE	Ensures a holistic lens can be applied through a well-defined scope
5) ADDS VALUE	Conducted from a performance perspective, not just compliance
6) DOWNSTREAM LENS	Looks at the risks not just of the organisation, but also its customers' or citizens' risks and potentially other participants in the ecosystem
7) RESOURCED	Resourced, as appropriate, internally or externally with a PIA provider that meets applicable criteria
8) AVAILABLE	Is available to the public – particularly where public trust and confidence is valued

8. About Privcore

Privcore's team with over 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens. Privcore conducts privacy impact assessments, privacy health checks or audits, data breach prevention and recovery, privacy by design, builds privacy programs, provides advice, policies and conducts research into privacy and cybersecurity.

Annelies Moens, CIPP/E, CIPT, FIP, FAICD, CMgr FIML, is the International Association of Privacy Professionals (IAPP) Vanguard Oceania 2023 Award recipient for demonstrating exceptional leadership, expertise and creativity in privacy and data protection. Annelies is also one of Australia's Superstars of STEM, selected in 2021-2022 for her widely recognised privacy expertise. She is a privacy professional practising since 2001 and founded Privcore, a privacy risk management consulting company.

She has led and conducted hundreds of privacy consulting deliverables globally. She is a former President of the International Association of Privacy Professionals which she co-founded in Australia and New Zealand in 2008. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She also has extensive privacy regulatory experience and resolved hundreds of privacy complaints whilst working at the Australian privacy regulator.


Annelies Moens
IAPP Vanguard
Oceania Award
2023
For demonstrating
exceptional leadership,
expertise and creativity in
privacy and data protection.
iapp