

Privacy Impact Assessments - Privacy by design

Table of Contents

Table of Contents	3
Executive summary	4
Key things to note:	4
Purpose	4
Scope	4
Privacy by Design	5
What is Privacy by Design?	5
Privacy Impact Assessment (PIA)	6
What is a PIA?	6
Purpose of the PIA process	6
Managing personal Information	6
What sort of project requires a PIA?	6
Examples of projects that may benefit from a PIA process	7
When should a PIA be undertaken?	7
How to undertake a PIA	7
When a comprehensive PIA is required	7
Process summary	8
Who should carry out a PIA?	8
Further advice and assistance	9
Appendix 1 - Checklist to decide if a PIA is necessary for a project?	10
Appendix 2 - Brief Privacy Analysis	12

Executive summary

Key things to note:

- Applying Privacy by Design (PbD) principles in projects promotes privacy and data protection from the start and helps Police meet our obligations for good stewardship of personal information.
- The Privacy Impact Assessment (PIA) process assists Police to comply with legislative and policy requirements for privacy, determine the risks and effects of a change or new project, and evaluate options to eliminate or mitigate potential privacy risks.
- Privacy Impact Assessments (PIA) will be undertaken on all projects that:
 - involve the personal information of our employees or the public, or
 - may affect whether an individual's reasonable expectations of privacy are met.
- Privacy issues and risks should be identified and analysed early - commence a PIA process contemporaneously with the business case work.
- View a PIA as a "living document" and review often to accommodate changes.
- Not all projects require a [full or comprehensive PIA process](#) but all projects must at least complete the 'Checklist' or the Brief Privacy Analysis (document below).

-

 [Privacy Impact Assessment - Brief Privacy Analysis.doc](#)

73 KB

Purpose

This chapter sets out Police expectations for adopting [Privacy by Design \(PbD\)](#) and undertaking [Privacy Impact Assessments](#) (PIAs) upon the creation of or changes to systems, structures or strategies that involve personal information.

Scope

This chapter applies to all Police employees and to personal information in whatever form it may exist including electronic and hardcopy.

Privacy by Design

What is Privacy by Design?

Privacy by Design (PbD) is an approach to projects that promotes privacy and data protection compliance from the start. It is a framework for the management of personal information and contributes to our vision of “trust and confidence of all.” Projects that involve new ways of dealing with or collecting personal information ought to include PbD principles. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.

The Privacy Act does not specifically require the adoption of PbD but applying the PbD principles will help Police meet our specific and general obligations for good stewardship of personal information.

The concepts within PbD are important when:

- building new IT systems for storing or accessing personal data
- developing legislation, policy or strategies that have privacy implications
- embarking on a data sharing initiative, or
- using data for new purposes.

The Information & Privacy Commissioner of Ontario (IPC) has taken a leading role in developing the privacy by design concept, establishing seven [‘foundational principles of privacy by design’](#).

The seven foundational principles are:

- Think about privacy at the beginning of your project
- Contemplate privacy as the default setting
- Privacy is embedded into the design of IT systems and business practices
- PbD will not compromise business goals
- Privacy protections should follow the lifecycle of the personal information
- Be open with all about the project or changes - contribute to trust and confidence
- Remember that individuals have rights and control over their information

Privacy Impact Assessment (PIA)

What is a PIA?

A PIA is a practical analytical process and report to:

- identify whether a proposed project is likely to impact either positively or negatively on the privacy of customers (the public) or employees affected by the project
- provide a framework for understanding the privacy risks and contemplating strategies to mitigate or eliminate those risks within a project
- provide a reference point for future action as the project changes.

Purpose of the PIA process

The PIA process is designed to identify risks or potential risks to the integrity and security of personal information through changed or new business projects. A PIA may also provide assurance that a project contains limited or no risks to the business.

The PIA process assists Police to:

- comply with the provisions of the [Privacy Act 2020](#) and policy requirements for privacy
- determine the risks and effects of a change or new project, and
- evaluate options to eliminate or mitigate potential privacy risks.

Importantly PIAs contribute to maintaining our vision of “trust and confidence of all”.

Managing personal information

Police is legally obliged to look after personal information in accordance with the Privacy Act 2020.

In addition to compliance with the law, personal information held by Police is an important strategic asset in the delivery of ‘[Our Business](#)’. Good stewardship of personal information will help to maintain a high level of trust and confidence by all people.

Good stewardship of personal information will be enhanced by undertaking a [comprehensive PIA](#) or at least a Brief Privacy Analysis (PDF below) when a new project or a new way of handling personal information may affect any individual’s privacy either negatively or positively.

-

[Privacy Impact Assessment - Brief Privacy Analysis.doc](#)

73 KB

What sort of project requires a PIA?

Police expects that a Privacy Impact Assessment (PIA) will be undertaken on all projects, big or small, that:

- involves the personal information of our employees or the public, or
- may affect whether an individual’s reasonable expectations of privacy are met.

Examples of projects that may benefit from a PIA process

- A major change project to introduce a new business process and supporting IT tools, for example switching from requiring clients to fill in paper forms, to enabling them to access Police services and information on line.
- Developing website or mobile applications that collects names or other personal data and that allows Police or customers to share information.
- A policy change, or new legislation, that requires sharing of personal information between different agencies, or collecting new information from individuals.
- The introduction of increased sharing protocols by allowing electronic access to personal information, to our people, other agencies or the public.
- Outsourcing a business or IT service where personal information is to be held or processed off-site or off-shore - or may be accessible to a host provider (for example using a cloud based service to store or process personal information).

When should a PIA be undertaken?

When designing or undertaking a project that includes personal information there should be an early identification and analysis of privacy issues and risks. A good point to commence a PIA process is contemporaneously with the business case work.

It is desirable to view a PIA as a “living document” rather than a once only view. As the project accommodates changes the PIA ought to be revised to reflect new positions and consequential privacy issues.

How to undertake a PIA

Not all projects will require a [full or comprehensive PIA process](#) but all projects must at least complete the ‘[Checklist](#)’ (see Appendix 1) or the Brief Privacy Analysis (document below, or Appendix 2). These will assist the project team by:

- informing the decision whether to prepare a comprehensive privacy impact report
- defining resource requirements (such as the skills that might be needed by an assessor, whether the task is small or large)
- suggesting terms of reference for the assessment

-

 [Privacy Impact Assessment - Brief Privacy Analysis.doc](#)

73 KB

A Brief Privacy Analysis should not be relied upon as the definitive risk and assurance process for all projects.

A PIA or at least a Brief Privacy Analysis must be a part of the project documentation used to seek project or budget approvals.

When a comprehensive PIA is required

If after completing a '[Checklist](#)' or 'Brief Privacy Analysis', it is desirable to undertake a more comprehensive PIA, consider the guidance on the [Office of the Privacy Commissioner's website](#):

- Part 1 - Deciding Whether To Do A Privacy Impact Assessment
- Part 2 - How To Do A Privacy Impact Assessment

These three templates on the [website](#) are also useful:


- Template 1 - Brief Privacy Analysis
- Template 2 - A Privacy Impact Assessment
- Template 3 - Risk and Mitigation Table

-

 [Privacy Impact Assessment - Brief Privacy Analysis.doc](#)

73 KB

Process summary

Stage	Description
1	Decide whether the project is one that requires a PIA ? Use the Checklist at Appendix 1 as an aid - if you answer "Yes" to one or more of the features listed there, it is highly likely a PIA will be necessary.
2	If you are unsure of the extent of known risks and responses to them, complete the Brief Privacy Analysis (Appendix 2)
	-
	<p> Privacy Impact Assessment - Brief Privacy Analysis.doc 73 KB</p> <p>Your brief analysis will help you decide whether more work is required perhaps in the form of a comprehensive PIA.</p>
3	If you believe a comprehensive PIA process is necessary consider the guidance on the Office of the Privacy Commissioner's website and/or consult with Police's Chief Privacy Officer .

Who should carry out a PIA?

The completion of a PIA does not always require a privacy specialist, Police's privacy officer or lawyer. If a project is particularly complex or the proposed use of personal information is significantly different to the usual status quo, it is worth engaging support (either internal or external) with the requisite expertise to either lead or assist with the assessment.

It is essential that particular project and other relevant staff contribute to the assessment. If an external specialist is engaged to complete a PIA it is crucial to the integrity of the assessment that our institutional knowledge is accommodated in the gathering and analysis of the project.

Police staff involved in a project need to be available to assist with the PIA process.

Further advice and assistance

For advice and assistance with PIAs and the process contact the [Chief Privacy Officer](#).

Appendix 1 - Checklist to decide if a PIA is necessary for a project?

(Download a **Word version** of the checklist for editing).

-

 Version 1 2017

48.5 KB

A one page check sheet to assist with identifying if a Privacy Impact Assessment (PIA) is required in order to 1) identify the impact of a new project on the privacy of customers (the public) or employees affected; 2) to provide a framework for understanding the privacy risks, 3) set out mitigations to manage the risks within a project and; 4) to provide a reference point for future action as the project changes.

PROJECT FEATURES THAT MAY INVOLVE PRIVACY RISKS	Y	N
Information Management Generally		
A substantial change to an existing policy, process or system that involves personal information		
Collection		
A new collection of personal information (for example, information about location)		
A new way of collecting personal information (for example, collecting it online)		
Storage, security and retention		
A change in the way personal information is stored or secured		
A change to how sensitive information is managed		
Transferring personal information offshore or using a third-party contractor		
A decision to keep personal information for longer than you have previously		
Use or disclosure		
A new use or disclosure of personal information that you already hold		
Sharing or matching personal information held by different organisations or currently held in different datasets		
Individuals' access to their information		
A change of policy that results in people having less access to information that you hold about them		

A change of process that enables an additional or new way to access information held by an agency		
Identifying individuals		
Establishing a new way of identifying individuals (for example, a unique identifier, a biometric, or an online identity system)		
New intrusions on individuals' property, person or activities		
Changes to your premises involving private spaces where clients or customers may disclose their personal information (reception areas, for example)		
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them (for example, introducing new conditions for a licence)		

Appendix 2 - Brief Privacy Analysis

Download the Brief Privacy Analysis used to determine or confirm whether a full or comprehensive Privacy Impact Assessment is required.

-

[Privacy Impact Assessment - Brief Privacy Analysis.doc](#)

73 KB

Printed on : 09/06/2022