basic education

Department:
Basic Education
REPUBLIC OF SOUTH AFRICA

Privacy Impact Assessment Manual

Contents

Executive Summary

What is a Privacy Impact Assessment (PIA)?

It is a process to assess and manage privacy impacts of a project, policy, programme, service, product or other initiative which involves the processing of personal information.

Why is a PIA performed?

The primary purpose is to identify risks to privacy and ways of dealing with those risks and to ensure compliance with the Protection of Personal Information Act, 2013 (POPIA) and its Regulations.

When is a PIA performed?

Whenever a department is developing or changing a system, project, program or activity to determine whether personal information will be processed (that is collected, used, retained, disclosed, secured or disposed of).

Who performs a PIA?

A PIA team under the leadership of a person who understands POPIA.

How is a PIA performed?

- By conducting a preliminary assessment to establish whether personal information is processed.
- If personal information is processed proceed to analyse the project and its privacy impacts.
- Draft a PIA report that:
    - either concludes that all privacy impacts (risks) are sufficiently addressed by appropriate and reasonable technical and operational measures; or
    - include recommendations to address the privacy impacts to ensure that the project will comply with POPIA's requirements.

Approval

The Director General (or the delegated authority) should either approve the recommendations contained in the PIA report or record that the privacy risks are accepted.

1. Introduction

The Department of Basic Education is committed to the protection of privacy guaranteed by the Constitution[1] which is given effect to by the **Protection of Personal Information Act, 2013 (POPIA).**

The Information Officer must ensure that a preliminary assessment is conducted when personal information (**PI**) is processed.[2]

This manual gives step-by-step advice on how to perform a **Privacy Impact Assessment** (**PIA**) to ensure compliance with **POPIA**. This must be read and used with the **Privacy Impact Assessment Template.** The template may be altered and/or supplemented to suit the unique needs of the department.

The departments routinely perform broad risk management activities and develop risk profiles related to their programs and activities. If the department undertakes a project which impacts on privacy a **PIA** must be performed.

For the purposes of this manual (i) "**project**" refers to any activity involving the processing of **PI**, which includes new and any changes to, a policy, program, process, service delivery model or an Information Technology (**IT**) system; and (ii) "**processing**" refers to the collection, use, retention, disclosure, security and disposal of **PI**.

The departments should create administrative linkages between **PIAs** and other risk mitigation tools and integrate **IT** threat and risk assessments with **PIAs**.

PIAs are to be embedded in a governance model that supports the implementation of the results of any assessment.

Privacy requirements must be integrated into each Chief Directorate/Directorates management systems and processes. Chief Directorate/Directorates are to be held responsible for compliance with **POPIA's** conditions and must proactively drive the inclusion of privacy considerations into the design of their service delivery goals.

In the case of a multi-institutional **PIA**, the department and institution involved will be responsible for contributing to or completing the **PIA** in a manner that is consistent with the approach outlined by the lead department/ institution.

2. Why conduct a PIA?

A **PIA** is a legal requirement. It assists the department to identify the impact (actual or potential) that a proposed or existing project may have on an individual's privacy.

---

[1] Section 14 of the Constitution of the Republic of South Africa, 1996

[2] A preliminary assessment is required in terms of Regulation 4 of the Regulations pertaining to the Protection of Personal Information Act, 2017.

Privacy is about the right of an individual to be left alone. There are two main but overlapping types of privacy that can be subject to different types of intrusion namely, **physical** or **informational** privacy.

Physical privacy is the ability of persons to maintain their own physical space or solitude. Intrusion can come in the form of:

- unwelcome searches of a person's home or personal possessions;
- bodily searches or interference;
- acts of surveillance; and
- the taking of biometric information.

Informational privacy is the ability of persons to control, edit manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of:

- collection of excessive personal information;
- disclosure of personal information without consent and misuse of such information;
- collection of information through the surveillance or monitoring of how people act in public or private spaces; and
- through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

Privacy risk is the risk of harm arising through an intrusion into privacy. All potential privacy risks are to be identified and mitigated.

The extent of a **PIA** will depend on the complexity of the project. Adapt the process to suit the needs of the project.

The benefits of a **PIA** include:

- ✓ Confirmation of the legal authority of the project to process **PI**;
- ✓ Demonstrating due diligence and evidence of compliance to support informed decision-making during the development of the project. This information is important in the event of a privacy breach or complaint to the Information Regulator.
- ✓ Assuring individuals, other institutions, partners and management that best privacy practices are being followed.
- ✓ Promoting better decision-making and a culture of privacy within the department.
- ✓ Improving transparency and better individual awareness, understanding and trust of the department's information management practices.
- ✓ Improving operational efficiencies by minimising excessive and unnecessary processing of **PI** and identifying simpler and less costly solutions upfront.

3. When to conduct a PIA?

A **PIA** must be conducted whenever the department is developing or amending a project which involves the use of **PI**, such as:

- An **IT** system for storing and accessing personal information
- A data sharing initiative where two or more departments/organisations seek to pool or link sets of personal information;
- A proposal to identify people in a particular group or demographic and initiate a course of actions;
- Use existing data for a new and unexpected or more intrusive purpose;
- A surveillance system or the application of new technology to an existing system (for example adding Automatic number recognition capabilities to existing CCTV);
- A new database which consolidates information held by separate government departments;
- Policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring

Even if it is thought that no **PI** is involved, it is recommended that **part A** of the **PIA** template is completed to ensure that the project has been accurately assessed.

A **PIA** must be done as early as possible when the project is developed and designed.

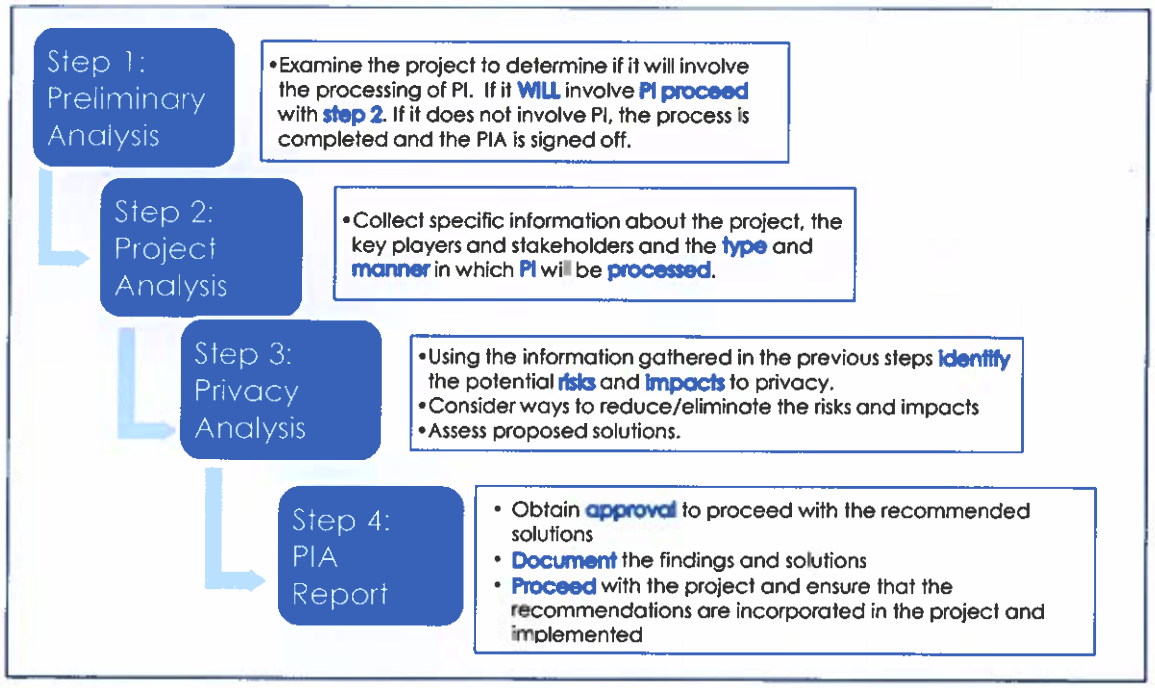
4. Who should initiate and conduct a PIA?

The line manager responsible for the project must sign off on the **PIA** and must lead the **PIA** team.

An effective **PIA** will require consultation with and the involvement of various persons who have specialised roles, expertise and insight into the project. The **PIA** team should have expertise in:

- ✓ policy development;
- ✓ operational program and business design;
- ✓ technology and systems;
- ✓ risk and compliance analysis; and
- ✓ access to information and privacy.

5. Methodology



5.1 Step 1: Preliminary Analysis

The first step is to determine if the project involves the **processing** of **PI**. This may be done by completing a **Preliminary Analysis Questionnaire** (**part A** of the **PIA** template).

Processing is defined in section 1 of **POPIA** as:

> *"**any operation or activity** or any set of operations, whether or not by automatic means, **concerning personal information**, including—*
>
> *(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;*
>
> *(b) dissemination by means of transmission, distribution or making available in any other form; or*
>
> *(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;"*

Personal Information is defined in section 1 of **POPIA** as:

> *information relating to an* ***identifiable, living, natural person****, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—*
>
> *(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;*
>
> *(b) information relating to the education or the medical, financial, criminal or employment history of the person;*
>
> *(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;*
>
> *(d) the biometric information of the person;*
>
> *(e) the personal opinions, views or preferences of the person;*
>
> *(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;*
>
> *(g) the views or opinions of another individual about the person; and*
>
> *(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;"*

If the project involves the processing of **PI**, the project and impact on privacy will have to be analysed (steps 2 and 3) and a **PIA** report (step 4) compiled.

If the project does not involve the processing of **PI** there is no need to comply with **POPIA**. This conclusion must be documented as part of step 1.

The **PIA** should be completed as early as possible in the project (preferably at the design stage) to ensure that the results of the analysis are built into the project plan. If answers are unknown upon initial completion, revisit the **PIA** process to update the information as details become known.

Consider all aspects of the project such as:

- The media where information is recorded. For example paper records, e-mails, phone records, computer logs etc.
- Whether the information will be linked with previously processed PI. Linking information increases the potential of identifying an individual even if the information itself is not considered PI.
- Whether the information will be shared with others, either internally (within the department) or externally (with parties outside the project/ department).

The purpose of completing **part A** of the **PIA** template is to:

- ✓ give an explanation of the project's purpose, scope and key objectives;
- ✓ understand the information involved in the project, and whether or a not personal information will be processed;
- ✓ describe the types of personal information that will be processed;
- ✓ take a decision whether or not to proceed with the PIA process and document the reasons for the decision.

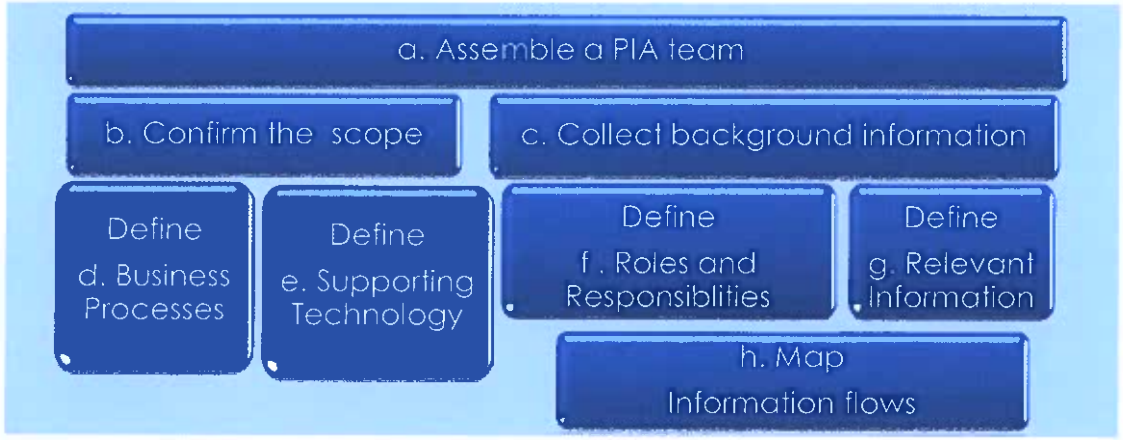
5.2 Step 2: Project Analysis

When **PI** is processed it is necessary to analyse the project to identify the potential impact it may have on privacy.

The **PIA** template includes a **Project Analysis Questionnaire (part B)**. Completion thereof will assist with defining and documenting the following:

- ✓ key characteristics of the project that may create privacy risks;
- ✓ activities and business processes involved;
- ✓ flow of **PI**, including identifying third parties (who will be doing what, when, how and why with the **PI**); and
- ✓ technology involved in the project.

It involves the activities depicted in the figure below:



a. Assemble a PIA team

The **PIA** lead must identify persons to complete the **Project Analysis Questionnaire**. This includes persons with knowledge in the following areas:

- ✓ **Business Processes**: relevant business processes, roles and responsibilities, and required resources;
- ✓ **Information Technology**: relevant technology policies, practices and standards;

- ✓ **Security**: relevant physical, technical and procedural security safeguards and requirements;
- ✓ **Information Management**: relevant policies, practices and standards;
- ✓ **Legal**: applicable privacy legislation, enabling legislation and other legal requirements, service level agreements, memoranda of understanding, contracts, etc.;
- ✓ **Procurement**: acquired or outsourced product and service solutions;
- ✓ **Risk Assessment**: risk assessment methodology;
- ✓ **Privacy**: issues, policies, practices, principles and applicable legislation; and
- ✓ **End-Users of Information**: employees and other parties who will use the systems or information collected or created by the project with expertise on practical implications.

Depending on the scope and complexity of the project, other areas, partners and stakeholders may need to be consulted.

b. Confirm the scope of the PIA

The scope of the **PIA** may not necessarily be the same as the scope of the project. If not adequately addressed in **part A**, revisit and explain what part/phase of the project the **PIA** covers and, where necessary for clarity, what it does not cover.

It is important to determine:

- whether the privacy risks and impact apply to all aspects of the project or to only some parts of the project; and
- whether the **PIA** will cover all associated business processes and technology.

If the project will be using pre-existing technologies or processes in the same way as they have been used before, which have already been analysed to assess the privacy impact, this does not have to be included in the **PIA**, merely refer to the related **PIA**.

c. Collect relevant background information

Collect all relevant project-related documentation, including information about:

- ✓ Business processes;
- ✓ Workflows;
- ✓ Information flows and business rules;
- ✓ Project management documentation;
- ✓ Previous privacy and security assessments;
- ✓ Training materials;
- ✓ Policies, procedures, business and IT design documents.

The available information will depend on (i) whether the project is creating something new or improving an existing process; and (ii) the timing of the **PIA**.

d. Define the relevant business processes

All applicable activities (business processes) that will be completed following implementation of the project must be recorded. This includes anything from technical processes (such as system back-ups or data processing), to policy and ongoing monitoring of a program, system or process.

The following must be documented:

- ✓ all existing and proposed activities associated with the project (paper-based as well as automated), including all parties, technology, and information associated with each activity;
- ✓ the current **IT** environment and how the project will impact it (e.g., create a new application);
- ✓ how the project's business processes will relate to other existing or planned programs, systems, or processes, including how information flows from the one to another; and
- ✓ if the project will change an existing program, system or process, how it will impact or alter current business processes, information flows, roles and responsibilities.

e. Define supporting technology

Identify and document the technology-related components of the project and determine if the technology used or developed in the project has privacy implications.

Take into account:

- How the technology will be used or developed to enable or support each step in the business process? Include existing systems, technologies and applications that the project will be using.
- How each technology will interact with PI?
- Who will have access to the PI using each technology?
- Whether there are any back-end processes in these technologies that auto-create records or store information in a way that is not immediately accessible by the user?

f. Define roles and responsibilities

The roles and responsibilities of all parties involved in the project must be identified and noted. In particular those who have access to **PI**.

Include all relevant partners and other third parties. Consider, apart from employees directly involved in the project the following categories of person who may have access to the **PI**:

- the public;
- clients/customers;
- employees in other Chief Directorates/directorates or institutions;
- IT employees (e.g., a system administrator);
- external legal counsel;
- other government bodies;
- partners, service providers, and vendors;
- auditors; and

- law enforcement agencies.

g. Define relevant information

Identify all types of records involved in each of the project's business processes (existing and proposed, paper and electronic) and describe the groups or types of information that will be processed in each business process or activity. Identify any special personal information associated with the business processes, such as medical information, criminal history, etc.

Where the project changes an existing program or system, determine whether it will alter the amount, type, sensitivity or source of personal information involved in the relevant business process.

h. Map the PI flows

Once the business processes, supporting technology and relevant information have been identified, determine how the **PI will** flow through the business processes and technology.

Map the flow of the **PI** in all formats from creation until final disposal by using diagrams and/or tables and descriptions that are readily understood.

This may include some, or all, of the following categories:

- source of information;
- collected by;
- collection method;
- purpose of collection;
- format of the information;
- purpose of use;
- used by;
- security control during information transfer;
- information repository format;
- storage retention site;
- purpose of disclosure;
- disclosed to;
- retention policy; and
- disposal or destruction policy.

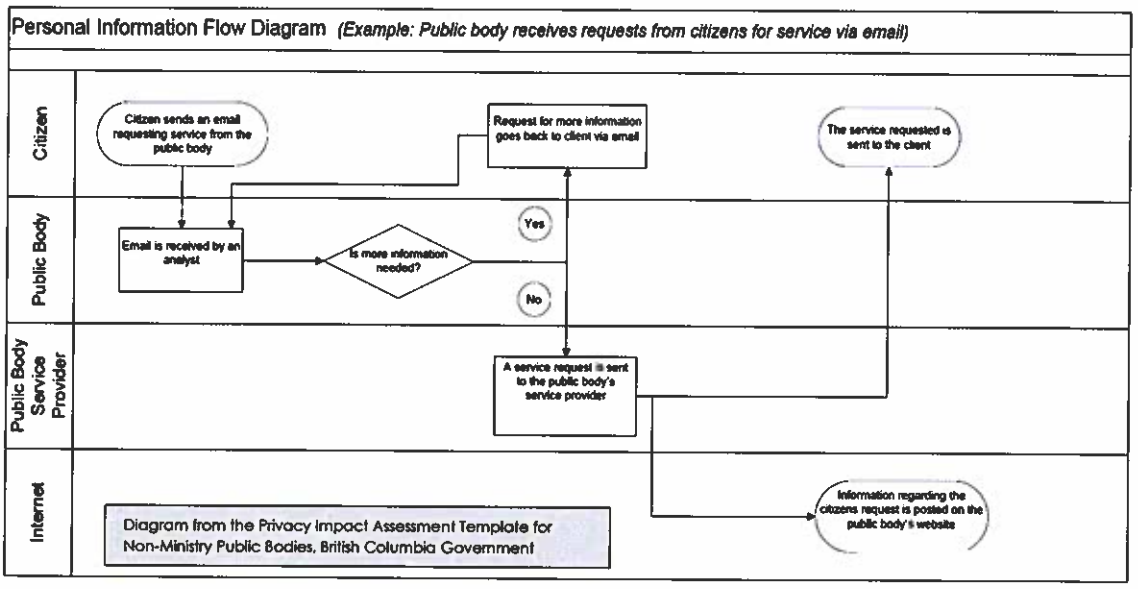
Map the flow of the personal information by using a **PI** flow diagram and/or a descriptive **PI** flow table.

Depending on the complexity of the project provide one general diagram/table for the project, and more specific diagrams/tables for particular components. If multiple parties will process **PI**, the diagram/table should identify how each party is involved in the project.

Table:

PI	COLLECTED	USED	RETAINED	SECURED	DISCLOSED	DISPOSED OF
	by? from? how? when? where? why? authority?	by? how? when? where? why? authority?	by? how? how long? where? why?	by? how? when? where? why?	by? to? how? when? where? why? authority?	by? how? when? where? why? authority?

Diagram:



Upon completion of step 2 the project analysis documentation should show:

- How **PI** will be **processed** including who is responsible and how technology will be used for each of these activities.
- Who will have access to the **PI** throughout its lifecycle, for what purposes and with what privileges. For example, who will process, browse or modify **PI** including program and **IT** staff, other programs providing services relevant to the project, and your partners and third parties.
- How **PI** will flow through existing and planned programs, systems or processes during each associated process.
- How and when **PI** will move beyond the custody of the department, that is, in the custody of a third party.

5.3 Step 3: Privacy Analysis

Step 3 involves a detailed examination of the privacy and related risks arising from the project and identifying and evaluating solutions to address these risks.

A **Privacy Analysis Checklist** (**part C** of the **PIA** template) will assist to determine and document whether the project will comply with **POPIA** and other privacy related legal requirements. If upon completion of **part C** it appears that the project will not be compliant, solutions must be identified to mitigate against the privacy impacts.

The solutions may be:

- technical (such as access control mechanisms, authentication mechanisms, encryption methods); and/or
- operational (management and operational controls e.g. policies or operational procedures).

Consult IT, risk management, security, legal and privacy experts to identify and evaluate potential risks and shortfalls in privacy protection.

At a minimum, the privacy analysis must cover the following areas and identify specific compliance actions taken or to be taken to meet with each area's requirements:

- Collection (authority, purpose, notification)- Conditions 2 and 6 of **POPIA**
- Use (authority, purpose) - Condition 3 of **POPIA**
- Disclosure (authority, purpose, sharing) - Condition 4 of **POPIA**
- Information quality (accuracy and correction) - Conditions 5 and 8 of **POPIA**
- Security - Condition 7 of **POPIA**
- Access - Condition 8 of **POPIA**
- Retention, Disposal and Destruction – section 14 of **POPIA**
- Privacy management (Accountability, training and audits) – Condition 1 of **POPIA**
-

Indicate any changes to the business requirements that have an impact on the system, software or program application and, consequently, may affect the current access controls and privacy practices related to the processing of PI.

Privacy impact

A privacy impact is the risk of harm arising through an intrusion into privacy. Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to individuals or institutions when not authorised;
- used in ways that are unauthorised, unacceptable to or unexpected by the person it is about;
- not kept securely; or
- processed without the appropriate legal authority.

Privacy impacts fall into two broad categories:

- Risks to **individuals** (e.g. identity theft, fraud, adverse impact on employment or business opportunities, reputational damage, embarrassment, distress or financial impacts); and

- Risks to **institutions** (e.g. financial, legal and reputational impact of privacy breaches and the consequences of failing to comply with **POPIA**).

All potential privacy risks are to be identified and mitigated.

Identify gaps and potential privacy impact

Use the **Privacy Analysis Checklist** to identify compliance gaps and the privacy impact and document the findings.

Consider existing privacy protection measures and planned actions that may apply to the identified requirements. If these measures are adequate document it as such. If not, this is a "gap" in privacy protection and an area of potential non-compliance and privacy risk.

Analyse findings

Analyse potential privacy risks and impact by taking the following into account:

- **Objective**: Start the analysis with the assumption that the desired outcome is to protect privacy to the greatest extent possible and to comply with **POPIA**.
- **Rationale for including PI**: Apply the concept of data minimisation and determine if there is a way to implement the project without processing **PI** or with less **PI**.
- **Privacy Impact**: Consider the potential harm associated with each compliance gap and identify the privacy risks or impact, if unable to mitigate or avoid them.

Understanding the privacy impact is central to the privacy analysis to identify action items to mitigate the privacy risks and make informed recommendations on how to implement the project to minimise its impact on privacy.

Identify privacy solutions

For each impact, identify solutions that will address possible compliance gaps and eliminate or reduce privacy risks. Some common solutions include:

- deciding not to collect, use or disclose particular types of personal information;
- creating retention periods that only keep information for as long as necessary and planning the secure disposal of information;
- implementing appropriate technological, procedural and physical security measures;
- ensuring that employees are properly trained and are aware of the potential privacy impact and appropriate privacy-protective measures to be followed;
- developing ways to safely anonymise and/or de-identify the information, where possible;
- producing guidance for employees on how to use new programs, processes and systems, and how and when it is appropriate to process **PI**;
- taking steps to ensure that individuals are fully aware of how their information is used and that they can contact the department for assistance, if necessary;
- selecting service providers/third parties that will provide a greater degree of security and ensuring that agreements are in place to protect the PI in the custody of the service providers/third parties; and
- producing information sharing agreements that clarify what information will be shared, how it will be shared and with whom it will be shared.

Each identified solution should be evaluated to ensure that it will either eliminate or reduce the impact to make the risk acceptable.

Identify action items

The analysis will allow the selection of the most appropriate solution/s.

Each impact requires:

- the identification of the specific actions;
- the responsible party for each action; and
- when it is to be implemented.

If the project is compliant record that no further action is required.

The solutions that need to be actioned are the "to do" list of items required to enable the project to protect privacy and comply with **POPIA**. This will be the mitigation strategy needed to minimise the project's privacy impact and should inform relevant employees as they proceed through the project. The outcomes should be integrated into the project plan.

5.4 Step 4: PIA report

The **PIA** process is completed by documenting the final conclusions and recommendations in a **PIA report (part D** of the **PIA** template).

This serves the following purposes:

- Decision-makers are provided with specific recommendations on how to address privacy impacts to make informed decisions about how the project should proceed;
- It demonstrates privacy due diligence; and
- Documents the results of the preliminary, project and privacy analysis that may be required for future reference.

List all additional documents that were used or are related to the **PIA.**

6. Approval

Appropriate approval should be obtained to implement the recommended privacy risk mitigation strategy in accordance with the department's approval process.

In the case of a multi-institutional **PIA**, indicate that the lead department/ government institution confirmed that the **PIA** was formally approved.

Approval of the **PIA Report** should be contingent on:

- the project's impact on privacy being fully and properly assessed;
- the decision-makers' understanding of the privacy risks and impact;
- the decision-maker/s approving:
  - ✓ the mitigation strategy to address the identified privacy impact; or

- ✓ the acceptance of the privacy risks, that is, a decision to take no action to address, and being aware of the consequences of such action.

7. Ongoing assessment

It is important to continue to assess the project's privacy risks and impacts as the project implementation progresses to determine if the privacy analysis and PIA report need to be updated.

Ongoing assessment is an essential part of identifying and mitigating new issues and changes impacting privacy that arise during implementation.

As the project is implemented:

- monitor progress of privacy-related activities to make sure they are appropriately completed;
- assess any changes to the project's implementation, that is, business process, information flows, roles and responsibilities to ensure that new privacy risks have not been created by these changes;
- evaluate mitigation measures to determine if they are effective when implemented; update or revise, if necessary;
- identify and assess new, outstanding and remaining privacy gaps and impact, and identify new action items required to address privacy risks;
- alert the project team and relevant decision-makers to any new privacy-related problems, and obtain appropriate approvals to address or accept the privacy risks and
- update or supplement the **PIA** documentation, if required, to document:
  - new privacy risks and impacts and how they arose;
  - their likelihood, harm and priority for action; and
  - the mitigation strategy to address the new privacy risks.

The project lead and other appropriate decision-makers should approve all significant changes impacting privacy and the acceptance of any privacy risks.

8. Concluding the PIA process

When concluding the **PIA** process ensure that:

- ❖ all privacy-related decisions, analysis and actions are appropriately documented;
- ❖ a copy of the **PIA report** and all supporting documentation are included in the project's files to ensure the project team and other key players can access the information; and
- ❖ transfer the privacy knowledge and **PIA** documentation to the appropriate parties, such as the program area, to enable ongoing privacy protection and the management of privacy risks once the program, process or system becomes operational.

Bibliography

1. Conducting privacy impact assessments code of practice 20140225 Version:1.0 ICO https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

2. Nymity Templates: Conduct PIAs for new programs, systems and processes.

3. Planning for Success: Privacy Impact Assessment Guide, Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf

4. Privacy Impact Assessment: OIPC NFLD Provides Expectations for Public Bodies http://www.oipc.nl.ca/pdfs/PIAExpectations.pdf

5. Template Privacy Impact Assessment for Non-Ministry Public Bodies, British Columbia Government http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments#templates

Additional resources

1. UK ICO Privacy Assessment Handbook Version 2.0

2. Privacy Impact Assessments Official Guidance - Privacy Office of the Department of Homeland Security https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf

3. Guidance on Privacy Impact Assessment in Health and Social Care - Health Information and Quality Authority (Ireland) https://www.hiqa.ie/system/files/HI_Privacy_Impact_Assessment.pdf

4. OIPC BC - Accountable Privacy Management in BC Public Sector (British Columbia, Canada) https://www.oipc.bc.ca/guidance-documents/1545

5. Privacy Impact Assessment Guide – Office of the Information Commissioner, Australia https://www.oaic.gov.au/images/documents/privacy/engaging-with-you/current-privacy-consultations/pia-guide/Guide_to_undertaking_Privacy_Impact_Assessment_-_public_consultation_draft.pdf

SIGNED ON BEHALF OF THE DBE ON BY:

DR G WHITTLE
ACTING DIRECTOR-GENERAL
DEPARTMENT OF BASIC EDUCATION
DATE: 17/11/21