Data Protection Office

Volume 6

Guidelines on PRIVACY IMPACT ASSESSMENTS

Mrs Drudeisha Madhub
Data Protection Commissioner

Tel No: 201 3604
Help Desk: 203 9076
E-mail: pmo-dpo@mail.gov.mu
Website: http://dataprotection.gov.mu

Table of Contents

INTRODUCTION

I. What is a Privacy Impact Assessment (PIA)?

A PIA is a methodology used to assess privacy risks to living individuals in the processing of their personal data including collection, use and disclosure of information. The reasons which may prompt an organisation to undertake a PIA are as follows:-

- Risk and Commercial Strategy Management
- Cost effectiveness
- Appropriate solutions
- Business Credibility
- Ascertaining legal compliance.

Projects with privacy implications require a full-scale privacy impact assessment (PIA) process.

A small-scale PIA or a large-scale PIA may be conducted depending on the size of the project. Because projects may be essentially different, a methodology should be devised that fits the specific requirements of the project, is explicit and as resource-intensive as is appropriate in the circumstances.

II. Compliance checking and data protection audit

A PIA needs to be distinguished from a data protection audit. Normally, a PIA should not be conducted on a project that has already been implemented. A PIA is best completed at a stage where it can genuinely contribute to the development of a project. Carrying out a PIA on an already existing project runs the risk of raising unrealistic expectations amongst stakeholders during consultation, unless there is a genuine opportunity to alter the design and implementation of a project.

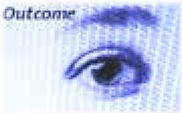
A data protection audit is more appropriate for existing projects. An audit is valuable in that it either confirms that data protection principles are being complied with, or highlights problems that need to be addressed. A PIA aims to prevent problems from arising. A PIA is broader than an audit of compliance.

PIAs have been designed as a self-assessment tool for organisations and the Data Protection Office does not have a formal role in conducting them and/or approving any final report which is produced. However, the office is available for all assistance required.

III. Who is required to complete a PIA?

There is no legal obligation for any organisation to complete a PIA. However, this template has been developed by the Data Protection Office as a Guide for all data controllers.

IV. What should be the expectations and outcomes of an effective PIA process?



The aims of an effective PIA should be the:

- identification of the project's privacy implications;
- assessment of those implications from the perspectives of all stakeholders;
- identification and assessment of privacy-enhancing alternatives;
- Unavoidable negative impacts on privacy should be capable of justification by the business need that requires them; and
- documentation and publication of the outcomes.

V. Why should a PIA be conducted?

- To identify privacy risks to individuals and data protection compliance liabilities for your organisation through the PIA.
- To avoid expensive, inadequate "bolt- on" solutions.

VI. Privacy risks

Definition of 'privacy risks'?

The massive increase in the collection, storage, use and disclosure of personal data, and the advent of intrusive technologies, are potentially harmful to individual privacy.

Privacy risks may be subdivided into two categories:-
i. Risks to the individual's privacy rights, or loss, damage, misuse or abuse of their personal information.
ii. Risks to the organisation as a result of:

- a failure to meet public expectations on the protection of personal information;
- retrospective imposition of regulatory conditions;
- low acceptance rates or poor participation in the scheme from the public and partner organisations;
- the costs of redesigning the system or retro-fitting solutions;
- collapse of a project or completed system;
- withdrawal of support from key supporting organisations due to perceived privacy harms; and/ or
- failure to comply with the law, leading to:
  - » enforcement action from the regulator; or
  - » compensation claims from individuals.

Recognising privacy risks

Any collection, use or disclosure of personal information is a potential risk to personal privacy. Sometimes those risks are not obvious and as a result they are easily overlooked or not adequately addressed to.

If the project design reflects a good understanding of privacy issues, it is possible that the participants in the consultation processes may agree to the design. However, because of project complexities and the diversity of interests among stakeholders, the consultation processes may sometimes create the need for parts of the project and its design to be re-considered.

This section provides some guidance on the type of risks, impacts and vulnerabilities you might look for when designing a project or conducting a PIA.

Broad personal information issues, including:

- **The nature of the personal information.** This could include "sensitive personal data" as defined by the Data Protection Act 2004, but also personal financial information, family structures, personal email addresses, information about persons considered "at risk", travel plans etc.
- **The quality of personal information.** This includes characteristics of the information itself, such as accuracy, relevance and adequacy. The more personal information moves from its original context, the greater the likelihood it can be misinterpreted. The quality of information also raises questions about data matching and mining, whether you are matching like with like and the number of false matches which may be produced.

- **The meaning behind terms used in personal information.** This takes into account that terms used can be context or sector specific. Variations in meaning of apparently similar terms may give rise to misunderstandings or error which in turn could result in harm or disadvantage to the individual. This area would also include examining metadata attached to personal information.
- **The retention, deletion and destruction of personal information.** How long do your business needs require retention of information? Are there legal obligations to dispose of or retain data? Do you need to keep information to counter legal claims or for audit and inspection purposes? Can your organisation make better use of ‘soft deletion’, where after the original purpose has been met, access to the information is much more tightly controlled until the organisation can permanently delete it?
- **The protection of personal information.** This includes the effectiveness of privacy protections. An effective privacy protection regime requires all of the following to be in place:
  - » clear specifications of privacy protections;
  - » clear prohibitions against breaches of protections;
  - » clear sanctions or penalties for breaches of protections;
  - » mechanisms in place to detect and report breaches; and
  - » resources for investigating breaches and applying sanctions.

Issues around identification of the individual, including:

- the multiple use of different identifiers;
- the denial of anonymity, identifying individuals where it is only necessary to authenticate rights to benefits, access and services;
- identifiers that directly disclose personal data, for example embedded date-of-birth;
- identifiers linked with authenticators, such as credit card number plus additional details, because that creates the risk of identity fraud and in extreme cases even identity theft; and
- the use of biometric identifiers.

Function creep, beyond the original context of use, in relation to the use of personal information or the use of identifiers.

Registration and authentication processes, including the burden such processes impose, their intrusiveness, and the exercise of power by government over individuals.

Surveillance, whether audio, visual, by means of data, whether electronically supported or not, and whether the observations are recorded or not.

Location and tracking, whether within geographical space or on networks, even where it is performed incidentally, and especially where it gives rise to a record.

From the perspective of privacy protection, there are considerable privacy benefits in decentralisation rather than centralisation. The benefits include:

- reducing the risk of function creep;
- enabling the application of access controls;
- encouraging a focus on relevancy;
- reducing the misinterpretation of data due to a loss of context; and
- increasing the likelihood of prompt data destruction when it is no longer required.

Where a project involves centralising information, it is important that there is clear justification. Further, those who want to use information in a more speculative manner (such as ‘statistical analysis’, ‘management reporting’ and ‘data mining’) need to be challenged for greater detail, and to show that benefits will be achievable. Once a case for centralisation has been established, it is necessary to identify, assess and balance the disadvantages.

Intrusions into the privacy of the person, especially compulsory or pseudo-voluntary (such as in employment relationships), yielding of tissue and body-fluid samples, and biometric measurement. It is highly advisable to document the issues which are identified.

Persons at risk and vulnerable populations
Some people, in some circumstances, face particularly serious risks if their personal data is disclosed. This applies especially to their physical location or data that may result in disclosure of their physical location. It may also apply to, for example, health care or financial data. Useful generic terms for people to whom this applies are ‘persons at risk’ and ‘vulnerable populations’.

Categories of persons whose physical safety is at risk include:

- **people who are under the direct threat of violence, including:**
  - people concealing themselves from previous criminal associates;
  - victims of domestic violence;
  - protected witnesses;
  - people who have been the subject of threats to their safety.

- **celebrities, notorieties and VIPs**, including:
  - politicians;
  - entertainers and sportspeople;
  - people ‘in the public eye’, such as lottery winners; or
  - those who publicly promote controversial views.

- people in security-sensitive roles, such as:
  - national security operatives;
  - undercover police;
  - prison wardens;
  - staff in psychiatric institutions.

Even where physical safety is not under threat, care may still be needed in respect of ‘vulnerable populations’, some of whom may find it difficult to exercise control over their personal data. Examples might include younger children or adults who lack capacity to provide consent. Your organisation might also want to consider the difficulties faced by individuals who are homeless or ex-detainees. Certain health conditions might also put individuals at risk if inappropriately disclosed.

Issues around the exercise of rights by individuals, such as whether personal information can be quickly and expediently identified, accessed, corrected or deleted. You should also consider whether an individual is disadvantaged in any way if they choose to assert their rights.

Future economic and social developments can also be considered.

Relevant legal considerations need to be taken into account, including liabilities that may arise and changes to regulatory impositions which may be necessitated by the project or by the public reaction to your project.

The conclusions regarding design features should be documented in the 'issues register', and provided to the project team as a whole. This is described in the later activities of the consultation and analysis phase.

VII. Identifying privacy solutions

Once you have identified and assessed the privacy risks your project presents, you need to consider what action you intend to take in relation to each risk.

PRIVACY SOLUTIONS

At this stage you have three options:

- accept the risks, impacts or liabilities;
- identify a way to avoid the risks (a privacy impact avoidance measure); or
- identify a way to mitigate the risks (a privacy impact mitigation measure).

Accepting the risks
In some instances, because of the nature of the risks, impacts or liabilities, the chances of the risks being realised or the minimal impact they may have, it might be entirely appropriate to simply recognise and accept the privacy risks or certain aspects of the privacy risks. However, this must not be done simply as an alternative to taking action to address risk and must be considered carefully as an option. If considering this option, ensure that a record of the identified risk is made, along with the reasons for accepting the risk.

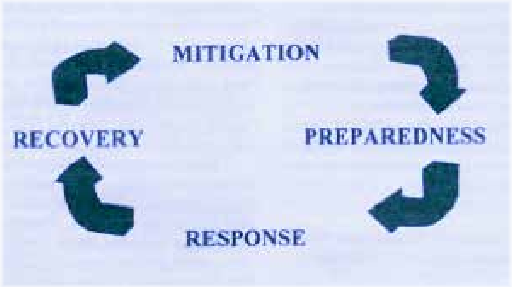
Privacy impact avoidance measures
An avoidance measure is a means of dissipating a risk. It refers to the exclusion of technologies, processes, data or decision criteria, in order to avoid particular privacy issues arising. Examples include:

- minimising the collection of personal information to what is strictly necessary;
- non-collection of contentious data-items;
- active measures to stop or block the use of particular information in decision making (a good example of this is ethnic monitoring forms being filled out anonymously when companies are recruiting);
- active measures to preclude the disclosure of particular data-items, for example screening or hiding of certain services which are being provided to the individual which might disclose other personal information;
- non-adoption of biometrics in order to avoid issues about invasiveness of people's physical selves.

Privacy impact mitigation measures
A mitigation measure is a feature that compensates for other privacy intrusive aspects of a design. A mitigation measure may compensate partially or wholly for a negative impact. Examples include:

- minimisation of personal data retention by not recording it;
- destruction of personal information as soon as the transaction for which it is needed is completed;
- destruction schedules for personal information which are audited and enforced;
- limits on the use of information which has been collected for a very specific purpose, with strong legal, organisational and technical safeguards preventing its application to any other purpose;
- design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers. Problems must be analysed, to devise acceptable avoidance and mitigation measures. The following suggestions are made about the process of problem analysis:
- The differing perspectives of the multiple stakeholder groups should be reflected.

- The focus of each impact and implication should be identified. For instance, what kinds of people or organisations will experience the various impacts, and under what circumstances?
- The justification for the feature that gives rise to the problem should be examined. For example, is the privacy infringement proportional to, or appropriately balanced with, any benefits gained from the infringement? And is it clear that the claimed benefits will actually arise?
- The circumstances in which the feature needs to be applied should be questioned. Is it appropriate for the data to be collected, used or disclosed in every instance, or can the data handling in question be limited to particular situations in which it is demonstrably relevant?



VIII. 11 questions for a PIA:-

Technology

(1) Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?

Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic. Technologies that are inherently intrusive, and technologies that are new and sound threatening, excite considerable public concern, and hence represent project risk.

In order to answer this question, considerations include:

- whether all of the information technologies that are to be applied in the project are already well-understood by the public;
- whether their privacy impacts are all well-understood by the organisation, and by the public;
- whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected; and
- whether all of those measures are being applied in the design of the project.

Identity

(2) Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?

Examples of relevant project features include a digital signature initiative, a multi-purpose identifier, interviews and the presentation of identity documents as part of a registration scheme, and an intrusive identifier such as biometrics. All schemes of this nature have considerable potential for privacy impact and give rise to substantial public concern and hence project risk.

Anonymity

(3) Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?

Many agency functions cannot be effectively performed without access to the client’s identity. On the other hand, many others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one’s identity, wherever feasible.

Multiple organisations
(4) Does the project involve multiple organisations, whether they are government agencies (eg in 'joined-up government' initiatives) or private sector organisations (eg as outsourced service providers or as 'business partners')?
Schemes of this nature often involve the breakdown of personal data silos and identity silos, and may raise questions about how to comply with data protection laws. This breakdown may be desirable for fraud detection and prevention, and in some cases for business process efficiency. However, data silos and identity silos are of long standing, and have in many cases provided effective privacy protection. Particular care is therefore needed in relation to preparation of a business case that justifies the privacy invasions of projects involving multiple organisations. Compensatory protection measures should be considered.

Data
(5) Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?
Section 2 of the Data Protection Act identifies a number of categories of 'sensitive personal data' that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings.

There are other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can enable identity theft.

Further important examples apply in particular circumstances. For example, the addresses and phone-numbers of a small proportion of the population need to be suppressed for national security reasons.

(6) Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?
Examples include intensive data processing such as welfare administration, healthcare, consumer credit, and consumer marketing based on intensive profiles.

(7) Does the project involve new or significantly changed handling of personal data about a large number of individuals?
Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them.

(8) Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?
This is an especially important factor. Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data.

Exemptions and exceptions
(9) Does the project relate to data processing which is in any way exempt from legislative privacy protections?
Examples include national security information and also other schemes where some or all of the privacy protections have been negated by legislative exemptions or exceptions.

(10) Does the project's justification include significant contributions to public security measures?
Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. Yet there have been tendencies in recent years not to give privacy its due weight. This has resulted in tensions with privacy interests, and creates the risk of public opposition and non-adoption of the programme or scheme.

(11) Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?
Disclosure may arise through various mechanisms such as sale, exchange, unprotected publication in hard-copy or electronically-accessible form, or outsourcing of aspects of the data-handling to sub-contractors.

Third parties may not be subject to comparable privacy regulation because they are not subject to the provisions of the Data Protection Act or other relevant statutory provisions, where they are in a foreign jurisdiction, for example. Concern may also arise in the case of organisations within Mauritius which are subsidiaries of organisations headquartered outside the country.

Facing facts early

The key characteristics addressed here represent significant risk factors for the project and their seriousness should not be downplayed. It should also be remembered that the later the problems are addressed, the higher the costs will be to overcome them.

Perspectives to consider

It is important to appreciate that the various stakeholder groups may have different perspectives on these factors. If the analysis is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked. It is therefore recommended that stakeholder perspectives are also considered as each question is answered.

In relation to the individuals affected by the project, the focus needs to be more precise than simply citizens or residents generally, or the population as a whole. In order to ensure a full understanding of the various segments of the population that have an interest in, or are affected by, the project, the stakeholder analysis that was undertaken as part of the preparation step may need to be refined. For example, there are often differential impacts and implications for people living in remote locations, for the educationally disadvantaged, for itinerants, and for ethnic and religious minorities.

Applying the criteria

Once each of the 11 questions has been answered individually, the set of answers needs to be considered as a whole, in order to reach a conclusion as to whether the PIA is warranted. If it is, a conclusion is also needed as to whether the scope of the PIA should be wide-ranging, or focused on particular aspects of the project.

Criteria for privacy law compliance checks

Senior executives of government agencies and company directors must ensure that the operations for which they are responsible comply with all relevant laws. The purpose of this section of the handbook is to assist organisations in complying with privacy-related laws. The services of a legal professional with relevant expertise may be needed. If any of the following questions are answered “Yes”, then a privacy law compliance check should be conducted:

Does the project involve any activities (including any data handling), that are subject to laws or guidelines other than the Data Protection Act, for instance, industry standards, eg the BS ISO / IEC 17799:2005 Information Security Standard or the Computer Misuse and Cybercrime Act or the civil law?

Template For Privacy Impact Assessment Report

[project’s name:- ....]

[date/period:- ....]

<u>THIS DOCUMENT REPRESENTS A MODEL OR GUIDE ONLY.</u>

This document has been prepared only to assist you structure a Privacy Impact Assessment (PIA) Report. It is intended to be adapted to your circumstances, depending on the project in question. You can also reformat this document to suit your organisation’s style and project/ risk management methodology, and remove the instructional text.

Bear in mind that not all of this model document will be relevant to your project. For example, if a PIA is done for a significant upgrade or migration to a new system, or the conversion of information from paper to electronic format, and where none of the collection, use or disclosures are changed, you would not be required to answer all the questions about collection, use and disclosure, instead you should indicate in those relevant sections for instance, “the project represents no change in relation to personal information handling covered by this section”.

Not every project will require a PIA. PIAs being used only where a project is of such a wide scope, or will use personal information of such a nature, that there would be genuine risks to the privacy of the individual. PIAs will usually be recommended for instance with the advent of new legislations, new and intrusive technologies are being used, or where private or sensitive information which was originally collected for a limited purpose is going to be reused in a new and unexpected way.

Table of Contents

In the table below, fill in any acronyms used in your report, as well as definitions of any special terms that a lay person may not otherwise understand. Privacy-related terms have already been completed for you. Please consult the Data Protection Act for other relevant definitions.

Glossary and Acronyms

PIA	**Privacy Impact Assessment**
DPPS	**Data Protection Principles**

Personal information:-
Any information relating directly or indirectly to a living, identified or identifiable individual.

Sensitive Information:-
Any information concerning a data subject as follows:-

a. the racial or ethnic origin;
b. political opinion or adherence;
c. religious belief or other belief of a similar nature;
d. membership to a trade union;
e. physical or mental health;
f. sexual preferences or practices;
g. the commission or alleged commission of an offence; or
h. any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings;
is sensitive.

Part 1 Definition of a PIA Report

What is a PIA?

Privacy Impact Assessments (PIAs) provide an effective means of measuring the privacy challenges posed by a new project, whether it be legislative, policy-driven or technological.

PIAs are usually undertaken as part of a sound risk management strategy, to assess whether it is safe to proceed to the implementation phase of the project. A failure to properly embed appropriate privacy protection measures may result in a breach of the Data Protection Act or prohibitive costs may be incurred in finetuning a system to ensure legal compliance or address corporate social responsibility concerns about privacy.

Privacy impacts may be negative (privacy-invasive) and/or positive (privacy-enhancing). However, since privacy is a human right, privacy impacts may only relate to individuals, not organisations.

This PIA Report aims to describe and de-mystify the privacy-implications of a specific project, identify and analyse them, and make recommendations for minimising privacy intrusion, and maximising privacy protection – while ensuring the project's objectives are met.

What does this PIA cover?

Insert a comprehensive explanation of the scope of this PIA Report.

Methodology

Insert an explanation of your methodology in preparing this PIA Report.

For example you might make reference to the project documentation upon which the assessment in this report was based. Also mention who has been consulted in the preparation of this Report, both internally and externally. If you used an internal person or team to conduct the PIA, explain how you managed any conflicts of interest.

If you have done stakeholder and/or public consultation, explain here whether quotes taken from discussions are attributed only indirectly and in an aggregate manner, or whether they are directly attributed to individuals or organisations with their permission.

Also explain here on what basis you have assessed the likely community expectations about how privacy will be managed in this project. For example, whether you commissioned research, used research from other sources, or conducted public consultation.

Part 2 Description of the project

Overview of the project

Insert a brief overview of what the project is, in 2-3 paragraphs.

Details of the project

Project objectives

Insert an overview of what the project is intended to achieve. Clearly set out what public benefit is expected as an outcome of the project. The rationale of the project is important, as you may need to weigh the benefits of the project against the risks it may pose to individual privacy.

Project drivers

Insert an explanation for how and why this project came about. For example, a driver for a project might be to address recent concerns about the quality of customer service in your organisation, or for another project it might be a need to achieve efficiency savings. Other possible drivers include the implementation of government policy or legislation, or the advent of a new technology.

Project scope

Insert an explanation of the scope of the project, in terms of the organisations involved and the individuals likely to be affected.

For example the project may involve a number of different business units within your organisation, as well as other public sector agencies, private sector stakeholders, and service providers. The individuals affected might be your staff, your clients, or broader members of the public.

Project environment

Insert a description of the environment affecting the project. This may include the current legislative environment, social or political factors including current government policies affecting the project, or technological parameters.

Project operational details

Insert a detailed description of how the project will operate. The following should be included:

- IT design;
- legislation – current and proposed;
- policies, procedures, forms etc;
- how the project will be communicated to clients;
- the physical environment and staffing; and
- accountability – plans for review, oversight, audit.

Explain here if alternative methods of delivering the project objectives have been considered and discarded, and if so for what reasons.

Data flow diagram

Insert one or more diagrams to illustrate how personal information is likely to ‘flow’ as a result of this project. You might consider one version showing how things work now, and a second version showing how things are intended to work if the project is implemented according to its current design.

Data flow diagrams should show each business unit and organisation involved in the project, and show how personal information will move between those units. You may need an accompanying table to explain the diagram and provide more detail.

Collection and Use of Personal Information

For each organisation or unit involved in the project, outline:

- what personal information will be collected and used;
- whether the collection of the personal information is authorised by the Data Protection Act or any other law;
- how the information will be collected (e.g. on paper, by email, through online transactions, by CCTV, etc);
- what are the purposes for which the information will be collected and used;
- who will be providing the information (i.e. whether the subject of the information will be providing it themselves, or a third party such as another organisation);
- who are the recipients of the information;
- whether the subject of the information will be aware of the collection of their personal information;
- what notification will be given to the subject of the information about the collection;
- what are the consequences for the subject of the information if the requested information is not provided to you;
- whether the subject of the information will have any choice about the collection and use of their personal information; and
- the right of the subject of the information to access, correct and destroy the personal information collected and used by the organisation.

Disclosure of Personal Information

For each organisation or unit involved in the project, outline:

- what personal information will be disclosed;
- whether sensitive information will be disclosed;
- for what purposes the information will be disclosed;
- whether the purpose of disclosure is directly related to the purpose for which the personal information was collected in the first place;
- whether the subject of the personal information will be aware of the disclosure of their personal information for this purpose;
- whether the disclosure of the personal information is authorised by the Data Protection Act or other laws;
- whether other disclosures might also be contemplated from time to time (e.g. whether personal information might also be disclosed to a law enforcement agency on request); and
- whether any information will be transferred outside Mauritius.

Data Quality and Security

For each organisation or unit involved in the project:-

- outline how they will ensure that the personal information they collect, use or disclose is accurate, complete and up to date. This may include an explanation of any opportunity given to individuals to correct or update their personal information before it is collected, used or disclosed;
- what format the personal information will be stored in (e.g. paper, electronic);
- where the personal information will be stored and by whom;
- what security and access controls will secure the stored personal information from misuse, loss, unauthorised use or disclosure;
- how long it will be stored for; and
- how and when it will be disposed of.

Diagrams or tables may be useful to illustrate the security and access controls and audit measures to be used to protect the personal information. For example a diagram showing network structure, firewalls and the like may illustrate network security.

Part 3 Assessment of the project with regard to the Data Protection Principles (DPPs)

At each point, recommendations are made to maximise the privacy enhancing possibilities, and/or minimise the privacy invasive risks of this project.

Ranking your recommendations will allow your organisation to prioritise its response. Recommendations which aim to mitigate a high level of privacy risk should be strongly urged, even if the cost of implementing your proposed mitigation strategy is also high. However low-level risks which would generate a high cost to mitigate may be considered less important.

Insert an explanation of the Timeframe, Risk and Cost to implement rankings you have applied to each recommendation.

The Timeframes you set will need to be appropriate for your project. For example, you might set out a timeframe of Immediate = within 2 months; Short-term = 2-6 months; and Long-term = 7-12 months. Or Immediate = before tendering; Short-term = before the database design is finalised; and Long-term = before we 'go live'.

Risk refers to the level of privacy risk if the recommendation is not followed. You can use a simple scale like 'High', 'Medium' and 'Low'.

Cost to implement refers to the cost of implementing the recommendation, meaning the financial cost, the time or resources involved, and the opportunity cost in terms of the impact on achieving the project's objectives. You can use a simple scale like 'High', 'Medium' and 'Low'.

1. Anonymity, Necessity and Means of Collection of Personal Information

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation. An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. An organisation must collect personal information only by lawful and fair means.

Collection of sensitive information

An organisation must not collect sensitive information about an individual unless the individual has consented, or made the data public, or the collection is required under law, or an exemption applies.

2. Use and Disclosure

An organisation must not use or disclose personal information about an individual in any manner incompatible with the purposes for which such data has been collected and processed.

3. Data Quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

4. Data security

An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

5. Data disposal

An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

6. Access

If a request for access to a document is duly made, and any required fee has been paid, the applicant shall be given access to the document, unless it is an exempt document.

The organisation must take all reasonable steps to enable the applicant to be notified of a decision on the request as soon as practicable but in any case not later than 28 days after the request was received.

7. Correction

A person is entitled to request the correction or amendment of any part of a document where it is inaccurate.

8. Personal data should not be transferred outside Mauritius to countries with no adequate data protection safeguards subject to certain exceptions provided in the Data Protection Act.

Assessment

Insert your assessment of the project in relation to these principles. Identify privacy risks as well as privacy-positive features.

Recommendation

Insert any recommendations to mitigate the privacy risks or enhance privacy protection in relation to this principle, the time frame and the importance.

Part 4 Assessment of the project: the privacy control environment

This Part of the Report assesses what might be termed the privacy control environment.
The privacy control environment refers to the mechanisms by which privacy protection will be managed as part of the project, or throughout the organisation. This may include policies, procedures and structures which affect accountability for privacy compliance.

Openness
An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

Privacy Management Function

The privacy management function encompasses responsibility, awareness and resources. The privacy management function for a project should incorporate such matters as:

one or more officers with nominated responsibility and appropriate skills, a process or plan by which privacy risks are identified and rectified staff training, manuals and other resources, clear responsibility and processes for complaint-handling, regular audits to check compliance logging of access to personal information, internal sanctions for misuse of personal information.

Accountability
Public trust in a project will be established and maintained through transparency about the project’s privacy impacts, throughout the life of the project. Accountability for a project should incorporate such matters as: published assessment/s of the project’s privacy impacts; public consultation about the project’s privacy impacts; mechanisms for stakeholder and public input into the design of the project; independent oversight of the project; and reporting on the implementation of this PIA Report’s recommendations.

Assessment
Insert your assessment of the project in relation to this principle. Identify privacy risks as well as privacy-positive features.

Recommendation

Insert any recommendations to mitigate the privacy risks or enhance privacy protection in relation to this principle, the time frame and the importance.

Part 5 Conclusions

A summary of findings

Insert a summary or overview of the most significant findings, in relation to both identified privacy risks and identified privacy-enhancing features.

The critical recommendations

Insert an overview of the critical recommendations. This should identify which privacy risks can be mitigated by following actions recommended in this Report.

Are the privacy risks justified?

Insert an overview of which privacy risks cannot be mitigated, the likely public reaction to such risks, and whether the risks are outweighed by the public benefit in the project proceeding nonetheless.

Project Action Plan

Fill in the first four columns in the table below for each recommendation made. This segment of the PIA Report can then be extracted as an Action Plan for the project team to document acceptance or rejection of each recommendation, and manage implementation of the recommendations.

No.	Recommendation	Risk	Cost to mitigate	Time - frame	Whether accepted	Who assigned to	Current status

Designed and Printed by the Government Printing Department - November 2012