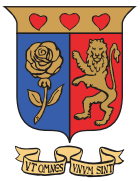
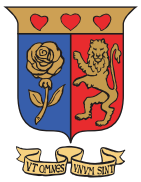


Strathmore University

Centre for Intellectual Property and Information Technology Law

Simplified Data Protection Impact Assessment

FOR SMALL ORGANISATIONS



Strathmore University

Centre for Intellectual Property and Information Technology Law

TABLE OF CONTENTS

Introduction

A Data Protection Impact Assessment (DPIA) is a systematic analysis of your data processing activities to help you identify and mitigate risks to people affected by your data processing activities.

The Kenya Data Protection Act requires that a DPIA be carried out where a data processing activity creates high risk to the rights and freedoms of a data subject.

Examples of high risk data activities include:

- Credit scoring
- Profiling of customers
- Processing involving sensitive personal data which is defined under the Data Protection Act to include: 'data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject'
- CCTV monitoring of a public area
- Database matching, particularly where third parties are involved
- Biometric data processing eg use of fingerprints or facial recognition software
- DNA processing
- Health data processing
- Services given to children or persons with mental incapacity
- Data processes that repurpose data previously collected for one purpose eg research using existing datasets

Steps For A Data Protection Impact Asssessment (DPIA)

STEP **01**
Description of the data processing activities

STEP **02**
Analysis of each processing activity

STEP **03**
Analysis of all the activities as a whole

STEP **04**
Risk determination

STEP **05**
Reporting to management.

STEP **06**
Monitoring and evaluation.

A NOTE ON THE ACTORS IN A DATA PROTECTION IMPACT ASSESSEMENT (DPIA)

The Data Protection Act uses the terms Data Subject, Data Controller, and Data Processor.

A Data Subject

A Data Subject is the person to whom data refers to. In this booklet, we use the term 'client' to refer to data subjects. Clients in a small organisation setting in a broad sense refers to anyone who is served by the organisation, including employees, customers, relatives of employees (e.g. for human resource functions), suppliers, partners, and contractors.

The Data Controller

The Data Controller is the person who decides, in a strategic manner, how data is processed. In many NGOs, this could be the management and at times the board. In an SME, it could be the management or the business owner.

The Data Processor

The Data Processor is any person who processes the data. In some instances, this is a different entity, for example where an SME uses an accounting system that is partly operated and fully owned by the accounting firm.

The Data Protection Act[1] defines processing to include:

> "(a) collection, recording, organisation, structuring;
>
> (b) storage, adaptation or alteration;
>
> (c) retrieval, consultation or use;
>
> (d) disclosure by transmission, dissemination, or otherwise making available; or
>
> (e) alignment or combination, restriction, erasure or destruction. "

From this definition, some examples of data processing work in small organisations include:

- processing the employee payroll
- analysing customers to learn something about their spending habits
- sending messages to customers
- taking details of clients who attend a training
- destroying old files containing client details
- archiving old files

1 See section 2 of the Data Protection Act

STEP ONE

Describing Your Data Processing Activities

WHAT

Describe the data you are processing. This could include: employee details, details of people who attend your legal aid clinic, lists of people who attend your community workshops, details of your clientele including their names, contact information, modes of payment et-cetera.

WHY

List down all the reasons you require the data you are processing. Some reasons could be: organisational management, human resource processes, programme management, accounting to donors.

HOW

For each data processing activity, describe the actual processing activity e.g. how the data is collected, recorded, organised, stored, and even used. Is the data ever shared, disseminated, altered, combined with others, archived, or destroyed?

WHERE

For each data processing activity, list all the physical and virtual places that data is processed.

WHEN

Describe when data processing takes place. Are there any activities that take place every month or every year or at the beginning of a contract?

WHO

List all the people and companies involved in the data processing.

Description of data processing activities will help the organisation to be aware of all data processing activities. It is also important in creating accountability structures. Although generally the management has overall responsibility over data processing activities, during this exercise, the organisation will identify the person in charge of the activity as well as others who are involved in the processing.

Table 1 shows an example of an accountability matrix:
Table 1: Responsibility matrix for a human resource management system

Data processing functions / Actors	Overall responsibility	Accountable for actual processing of data	Consulted in data processing	Informed of data processing activities
Business owner				
Management				
IT department				
Finance department				
Human resources department				
Technology / system provider				
Employees				

After going through the data protection impact analysis, the responsibility matrix may change. For example, you may realise that employees need to be consulted in data processing activities or that the IT department needs to be accountable for some data processing activities.

A NOTE ABOUT SPECIAL GROUPS

When analysing your data processing activities, pay special attention to vulnerable groups such as children. Increasingly, governments are requiring that any data processing that targets children be carried out under special conditions. For example, the UK has a Code[2] that requires organisations processing children's data to incorporate the best interests of the child. This includes taking into account the different ages of children and protect children from harmful use of data. In practice, an organisation processing children's data must make the processing child specific, and apply the data protection principles to the highest, for example, explain the purpose of processing the data in a very simple way. It must also provide avenues for parental controls, restrict nudging the children and make considerations for connected data for example where there are connected toys and devices.

2 ICO, 'Age Appropriate Design: A Code of Practice for Online Services' <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>

STEP TWO

Analysing your data processing activities

There are different tests you could use to assess the impact of your data processing activities. These include: principles analysis, the legitimate interest test, necessity and proportionality test, privacy by design and default test, rights analysis, profiling, and risk mitigation.

2.1 Principles Analysis

There are eight principles of data protection under the Data Protection Act. These principles are laid out and described in Table 2 below.

Table 2: Principles of data protection under the Data Protection Act, section 25

Privacy	Process data with regard to the privacy of individuals
Fairness & lawfulness	Be fair and transparent to clients whose data you are processing
Purpose	Have a specified purpose for processing data
Adequacy	Only collect what is sufficient for your specified purpose
Valid explanation	Explain to your client why you are collecting data on family or private affairs
Accuracy	Keep personal data accurate and upto date. Rectify or erase incorrect personal data
Retention	Do not keep data longer than necessary. Anonymise data that is no longer in active use
Transfer outside Kenya	Ensure data in your custody that is processed outside kenya is processed in countries with adequate data protection laws.

An organisation processing personal data should adhere to the principles of data protection set out in the Data Protection Act.

A basic step for a DPIA is to assess your data processing activities against the data protection principles. The queries in the principles test analysis include the following:

- Do you collect any data relating to private or family affairs?
- For each data point, e.g. name, location, date of birth, what is the specific reason for data collection and processing?
- What processes would have to be followed for the data to be used for other purposes?
- For each data form, e.g. a client enrolment form, is all the data collected relevant and necessary for the job it will be used for?
- Do you explain to clients why their data is being collected and how it is used?
- Is the client data in your possession accurate?
- Is data processed and stored securely?
- How long do you keep your client data?
- Do you archive data?
- What measure are taken to protect identification of clients when archiving data?
- Is any data destroyed?
- How do you communicate with your clients regarding their data rights?
- Is any of your client data processed or stored in servers outside Kenya? In which country? [3]

Some measures you would have to take after this analysis include:

- Redesigning data collection to include only relevant data for your purpose
- Explaining to clients your reasons for collecting and processing their data
- Creating mechanisms for your clients to review whether the data you have on them is accurate
- Reviewing your archiving protocols to ensure that archived data is secure and does not reveal personal information
- Destroying data that is no longer needed
- Reviewing contracts and services for storage and processing of data to ensure that data is stored in countries that have adequate data protection laws
- Periodically monitoring cybersecurity measures
- Training staff on data protection principles

3 For a more detailed set of questions for each principle, see Annex 1

2.2 Legitimate Interest Test

A legitimate interest is the basis for the collection of data. Some examples of such basis could include: an NGO collecting data of people who attended an activity for financial accountability, and an SME collecting client contact information for future communications.

Some of the questions to guide the legitimate interest test include:

- What are your data processing activities?
- What data is collected in each data processing activity?
- How long will the data be retained?
- If already collecting data, what data is not required?
- How do you ensure that the data collected is of good quality?
- For each data processing activity, why do you collect the data you collect? Is it in pursuance of a law? Is it for accounting purposes? Or is some data processing out of practise?

Once the reason for data processing has been established, steps that could be taken include:

- Where some of the data processing is unjustifiable, it should be stopped; and
- Where a decision is taken to halt data processing, create a plan for retirement of the data that was previously collected to mitigate against misuse of that data.

An organisation processing personal data should have justifiable reasons for processing the data.

2.3 Necessity And Proportionality Test

This test is complementary to the legitimate interest test. While you may have a legitimate interest for processing data, your interest needs to be balanced against the rights and interests of your clients.

Some important issues to include in the necessity and proportionality test include:

- What is the lawful basis (legitimate interest) for the processing?
- What data is required in order to achieve the legitimate interest?
- Which client rights are potentially affected by the data you collect?
- In the event of a data breach, how many persons would be affected?
- In the event of a data breach, what could be inferred from the data you have?
- How do you protect the privacy of not just your clients but everyone else to whom the data relates? List the measures taken.

After the necessity and proportionality analysis, some of the steps you may need to take include:

- Halting collection of unnecessary data
- Creating a plan for retirement of data that will no longer be necessary
- Introducing sunset clauses or expiry terms on data processing
- Creating notification procedures to communicate with clients in case of data breaches or any other events that they should know of
- Creating procedures for clients who may want to opt out of some data processing e.g. employees who may not want to declare their family
- Creating governance mechanisms such as data protection committees to periodically monitor data processing activities

Necessity asks the question, does your data processing go beyond your legitimate interest? Proportionality asks, are there any other ways to achieve the same result that would better protect your clients' rights and interests?

2.4 Profiling Analysis

Profiling is the automated processing of data for personal evaluation. If your organisation uses artificial intelligence (AI) or automation in data processing, you should carry out a profiling analysis. In a profiling analysis, describe the personal data analysed in the profiling process, the considerations taken in the automated process, and then assess the risk.

The Data Protection Act describes profiling as the use of automated processing to analyse or predict a person through their race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth, personal preferences, interests, behaviour, location or movements[4].

Questions for profiling test include:

- What data processing activities use automated processing? Describe them.
- Are there processes where decisions are made solely based on automated decisions?
- Are clients aware that automated decision making is used?
- Can clients appeal if they are dissatisfied with the automated decision?

Steps to take once the profiling analysis has been done could include:

- Creating procedures for human intervention/review of automated decisions
- Creating procedures for clients to appeal automated decisions
- Creating communication mechanisms to inform clients of automated decision making and available appeal procedures

The Data Protection Act protects your clients from decisions made only on the basis of automated decision making, including profiling. You can only use automated decision making:

- ***If it is for purposes of a contract where automated decision making is required in order to fulfil the contract***
- ***Where there is a law that safeguards the interests of your client or***
- ***Where your client has consented to use of automated decision making***

4 See section 2, Data Protection Act

2.5 Privacy By Design And Default Test

Privacy by design and default means incorporating privacy in the building, management, and operation of any given data processing system or activity. Privacy by design calls for incorporation of privacy during development of a system. Privacy by default means that once the system is in place, the highest standards of privacy should apply by default, without any input from the user.

Some guiding questions in considering privacy by design and default include:

- What is the data lifecycle in your organisation?
- What privacy measures exist in each stage of the data lifecycle?
- What are the privacy measures in the data processing system? Do they anticipate, identify, and prevent invasion of the system?
- Is data automatically protected once it is collected?
- Are the staff aware of privacy and data protection?
- How are privacy incidences e.g. breach reported and resolved?
- Are clients made aware of privacy incidences?

Once the privacy by design and default analysis is done, some measures to take could include:

- Reconceptualising privacy as a proactive, and not reactive practice during system design
- Including privacy by design and default analysis in the procurement of systems
- Creating and testing privacy measures where they do not exist in the data lifecycle
- Training staff on privacy and data protection to inculcate privacy in all organisation activities
- Creating procedures for communicating privacy incidences with clients
- Undergo privacy certification from privacy and security professionals
- Create privacy governance mechanisms such as creation of data protection committees and appointment of a data protection officer

An organisation processing personal data must incorporate privacy by design in its systems. For systems already in place, they should default to privacy even without any input from the user.

2.6 Rights Analysis

The rights analysis may complement the necessity and proportionality test as it considers the rights of data subjects in relation to the data processing activities. The rights analysis involves both privacy and data protection rights as well as other rights.

Table 3: Privacy rights under Data Protection Act, Section 26

Privacy rights	Description
Right to information	Clients should be informed on how their data is being used
Access to personal data	Clients should be able to view the data you have about them
Objection to processing	Clients have a right to oppose to all or part of their data being processed, and the organisation should provide means through which clients can make such requests
Correction of false or misleading data	You should provide mechanisms through which clients can request correction of false or misleading data
Deletion of false or misleading data	Clients can request deletion of false or misleading data from your records

Data processing activities should promote other rights of your clients and not expose the rights of your clients or their families.

Questions to guide the analysis include:

- Do you collect or process sensitive data such as people's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation?
- Can sensitive information be inferred from data that you have in your possession?
- How many people would be affected if the data you have was exposed?
- How would people be affected if your data is exposed- could sensitive details about their lives be revealed or inferred?
- Has your organisation suffered data breaches in the past?
- What are the threats to the data you hold?
- What technical measures have you put in place to protect against threats to the data?
- What are organisational measures re in place to protect the data from exposure?
- How are data subject rights incorporated in your data processing activities or in the data life cycle?
- Who makes decisions related to data requests from clients and others? Is it the system?
- What rights are affected in your data processing activities? This requires listing of other rights and not just privacy. Examples of rights that could be affected include rights of children, freedom of expression, freedom of association, economic rights, family rights etc.

Some steps to be taken after a rights analysis include:

- Creation or enhancement of procedures through which clients and others can access their data rights
- Incorporation of human intervention where client requests are automated (refer to profiling analysis)
- Establishment of data governance mechanisms eg a committee to consider complex requests from clients and others

STEP THREE

Analysis of all the activities as a whole

Analysing the data of all activities carried out enables the identification of risk which is used to flag down any existing vulnerabilities to the data collection, assessment, and storage systems. This helps in focusing on closing the privacy gaps that may be identified during the process. Key factors to consider during the overall analysis include:

- Systems and process: All the systems where data is collected, how data is shared across systems, and all actors within the organisation who access the data for various functions
- The data life cycle in the organisation: how data enters the organisation, how it is processed, how it changes, when it is retired, and how it is destroyed.
- Vulnerabilities of the data processing systems: scope, extent of data and impact of data breaches within and outside the organisation ecosystem.
- System security
- The extent to which the people in the organisation, as well as partners, understand and practice data protection
- Governance of data, including relationships with third party data processors, engagement with clients and public.

Once analysis of all activities is done, possible actions that may follow include:

- With regards to the data:
  - ◊ Consultation with clients whose data you possess
  - ◊ Collection of further data for accuracy of data
  - ◊ Merging datasets
  - ◊ Erasure or destruction of data that are no longer necessary or justifiable
  - ◊ Deleting of some datasets
  - ◊ Restructuring of organisation processes for more efficient data processing
  - ◊ Restructuring of data security protocols to enhance protection of personal data
  - ◊ Redesigning data processing systems to default to privacy
- For data governance:
  - ◊ Review of contracts with third party processors
  - ◊ Creation of data protection committees
  - ◊ Creation of data protection reporting hierarchies
  - ◊ Restructuring information security committees to undertake data protection tasks as well
  - ◊ Carrying out of system audits
  - ◊ Appointment of a data protection commissioner to oversee data governance
  - ◊ Training of all staff on data protection
  - ◊ Development of an internal data protection manual

STEP FOUR

Risk Determination

Risk determination is an assessment on the likelihood of a risk. Data processing comes with reputational, financial, and rights related risks. For example, data can be lost or stolen, anonymised data can be re-identified, and sensitive data can be leaked, leading to emotional damage.

Process in risk assessment can involve:

- identification of the risk
- development of a risk classification method
- establishment of mitigation measures to match the risk classification

Examples of risks include:

- system failure, which could result in data being unavailable or exposed for longer than necessary
- unauthorised secondary use of data
- corruption of data
- malicious interference by internal or external actors
- accidental human interference for example inadvertent copying, erroneous deletion
- natural disasters affecting physical infrastructure

Risk determination could either follow industry standards or be developed collaboratively in the organisation.

Below is an example of a risk identification matrix:

Severity of impact				
	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Figure 1: Risk Identification Matrix. Source: ICO

Once a data processing activity is determined to be either high, medium or low risk, the organisation needs to identify measures that will mitigate the risks. Examples of mitigation steps could include:

- Preventative measures such as:
  - Staff training to stop habits such as data sharing
  - Sunset clauses on data that does not require to be retained perpetually
  - User management
  - Separation of sensitive personal data from other data to spread the risk across different repositories
- Repressive measures such as
  - Monitoring processing operations to detect anomalies and breaches as soon as possible
  - Procedures for revocation of compromised credentials
- Corrective measures for example:
  - Backups with which status quo can be restored
  - Communication with clients and other affected people in event of a data breach

It is **important to note** that the Data Protection Act[5] provides that **where data processing risk is determined to be high**, you **are required** to **consult** the data protection commissioner **at least sixty days prior** to that processing.

5 Section 31(3) Data Protection Act

STEP FIVE

Data Protection Impact Assessement (DPIA) Report

Once a determination has been made, a DPIA report is prepared for consideration by management. It is important for management to deliberate on the DPIA for:

- **Overall accountability:** The management needs to be aware of all data processing activities as they have overall responsibility for data processing within the organisation.
- **Publication:** Although this is not mandatory, some organisations publish the DPIA for transparency.
- **Prior consultation requirement:** The Data Protection Act requires prior consultation with the Data Protection Commissioner, where data processing activities are determined to be high risk[6].

What Should Be Included In The DPIA Report?

The report will inform management of its compliance obligations and whether it has met provided regulatory specifications. Further, the report needs to inform management of any risks, threats, and measures that have been taken or need to be taken to minimize risk. It should contain:

- Description of all data processing activities
- Analysis of each activity and test used
- Overall analysis of all processing activities in the organisation
- A risk determination
- Recommendations on steps the organisation needs to take to comply with the data protection act and to mitigate risk for clients whose data they hold

6 Section 31(3) Data Protection Act

STEP SIX

Monitoring and Evaluation

Data protection is not a one-off activity[7]. Data practices in the organisation must be continually assessed to inculcate a culture of privacy and data protection within the organisation and with those the organisation interacts with.

Monitoring involves tracking data processing activities to anticipate incidences that could impact on the rights of clients. Evaluation means testing how well data protection practices are working.

Table 4: Monitoring and evaluation of the DPIA

Monitoring	Evaluation
Track data processing activities Identify data protection incidents Anticipate incidents Output: Recommend changes to management as appropriate	Examine the relevance of data protection mechanisms in the organisation. Analyse if data protection measures meet objectives of the Act. Output: Lessons and recommendations for future DPIA

Conclusion

In summary, a DPIA is the process through which an organisation describes their processing activities, assesses the risk those activities pose to the rights and freedoms of persons and puts in place measures to address those risks.

While a DPIA should be carried out prior to data processing, many organisations in Kenya will conduct the process on existing systems. We hope that this resource is useful in conducting your DPIA as well as increasing your knowledge on Kenya's data protection laws.

7 See European Commission (2017) Guidelines on Data Protection Impact Assessment (DPIA)

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Annex 1: Further questions for principles analysis

Fairness

- Can clients expect you to have the data you have on them, even if they did not read the information you provided them with?
- If consent is your basis for data processing, did you give an explanation before it was given? Was it freely given? How do you document that people gave it? How can they revoke their consent?
- Could the data you have on your clients generate chilling effects?
- Could the data you have, lead to discrimination?
- Is it easy for your clients to exercise their rights to access, rectification, erasure etc.?

Transparency

- Is the information you provide complete and easy to understand?
- How do you ensure that the information you provide actually reaches the individuals concerned?
- Have you tailored information to different audiences? e.g. children may require tailored information
- Where you have not provided information, how do you justify data collection or processing?

Purpose Limitation

- Have you identified all purposes of your data processing?
- Are all purposes compatible with the initial purpose for which data was collected?
- Is there a risk that the data could be reused for other purposes (function creep)?
- How can you ensure that data is only used for their defined purposes?
- In case you want to make available / re-use data for scientific research, statistical or historical purposes, what safeguards do you apply to protect the individuals concerned?

Data Minimisation

- Do the data you collect measure what you intend to measure?
- Are there data items you could remove without compromising your purpose?
- Do you clearly distinguish between mandatory and optional items in forms?
- In case you want to keep information for statistical purposes, how do you manage the risk of re-identification?

Accuracy

- Are the data of good quality for the purpose?
- How would inaccurate information affect your clients in your data processing?
- How do you ensure that the data you collect yourself is accurate?

- How do you ensure that data you obtain from third parties is accurate?
- Do your tools allow updating / correcting data where necessary?
- Do your tools allow consistency checks?

Storage Limitation

- Is there any law, e.g Data Protection Act, Insurance Act, Income Tax Act etc that defines durations for which you must keep data?
- How long do you need to keep which data? For which purpose(s)?
- Can you distinguish storage periods for different parts of the data?
- If you cannot delete the data just yet, can you restrict access to it?
- Will your tools allow automated permanent erasure at the end of the storage period?

Security

- Do you have a procedure to perform an identification, analysis and evaluation of the information security risks potentially affecting personal data and the IT systems supporting their processing?
- Do you target the impact on people's fundamental rights, freedoms and interests and not only on the risks to the organisation?
- Do you take into consideration the nature, scope, context and purposes of processing when assessing the risks?
- Do you manage your system vulnerabilities and threats for your data and systems?
- Do you have resources and staff with assigned roles to perform the risk assessment?
- Do you systematically review and update the security measures in relation to the context of the processing and the risks?

Strathmore University
Centre for Intellectual Property and Information Technology Law

Ole Sangale Rd, Madaraka Estate.
PO Box 59857-00200, Nairobi, Kenya.
Tel +254 (0)703 034612

Email: cipit@strathmore.edu
Website:www.cipit.strathmore.edu

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international
Canada

AUTHORED BY GRACE MUTUNG'U AND FLORENCE OGONJO.
EDITED BY MELISSA OMINO.