REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

GUIDANCE NOTE ON DATA PROTECTION IMPACT ASSESSMENT

GUIDANCE NOTE ON DATA PROTECTION IMPACT ASSESSMENT

Definitions

"Act" means the Data Protection Act, No 24. of 2019.

"Biometric Data" means personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition.

"Consent" means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

"Data Commissioner" means the person appointed pursuant to section 6 of the Act.

"Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data;

"Data Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

"Data Protection Impact Assessment" or "DPIA" means an assessment of the impact of the envisaged processing operations on the protection of personal data, as defined in section 31(4) of the Act.

"Office" means the Office of the Data Protection Commissioner as defined in sections 2 and 5 of the Act.

"Personal Data" means any information relating to an identified or identifiable natural person.

"Processing" means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as:

(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.

"Sensitive Personal Data" means 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.

1. INTRODUCTION

The Office of the Data Protection Commissioner (herein referred to as 'the Office' or 'ODPC') is a State Office in accordance with Article 260 (q) of the Constitution. The Office was established under Section 5(1) of the Data Protection Act No. 24 of 2019 (herein referred to as 'the Act'). The Act was introduced to give effect to Article 31(c) and (d) of the Constitution.

2. MANDATE OF THE OFFICE

The mandate of the Office of the Data Protection Commissioner derived from the Act and includes, inter alia:

(a) regulate the processing of personal data;

(b) ensure that the processing of personal data of a data subject is guided by the principles set out in section 25 of the Act;

(c) protect the right to privacy of individuals resident in Kenya;

(d) establish the legal and institutional mechanism to protect personal data; and

(e) provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act.

3. VISION

To enhance public trust and be an effective personal data protection regulator.

4. MISSION

Safeguarding data protection rights through provision of oversight, public awareness and promotion of self-regulation.

5. CORE VALUES

(a) To uphold Values of Public Service as set out in Article 10, and in Chapter Six of our Constitution;

(b) To act lawfully consistent with our Constitution, and within duties and responsibilities set out in the Data Protection Act 2019;

(c) Be consultative in style, transparent and responsive to all stakeholders;

(d) To observe the highest standards of impartiality, integrity and objectivity in leading data processing business while maintaining its independence at all times;

(e) To cause to have in place effective systems of internal controls for effective economical and proper performance of the functions of the Office.

6. BACKGROUND

The Data Protection Act, 2019 ("the Act") and Data Protection and Privacy Policy 2019 espouses the seven data protection principles, namely:

(i) Lawfulness, fairness and transparency - All personal data needs to be processed fairly and lawfully, and in a way that is completely transparent. Simply put, an entity is responsible for informing data subjects (natural persons) that they intend to collect data, how the data will be used and whether the data is to be passed on/disclosed to a third party and who the said third party is.

(ii) Purpose limitation - Data collection must be for a reason that is lawful and transparent, it must not be processed in a way that is at odds with the original purpose.

(iii) Data minimisation – Entities which collect data must make sure that the information collected is not excessive, given the purpose of collection. Therefore, the personal data should be adequate, relevant and not excessive.

(iv) Accuracy – Entities collecting data are required to ensure that information held is up-to-date and accurate, which requires a regular review of data held for the purpose of amending any out dated or inaccurate information. Individuals have the right to have inaccurate data about them erased.

(v) Storage Limitation – Data relating to a data subject must be deleted or anonymised once it has served its purpose, subject to the entity having any other grounds for retaining the information.

(vi) Integrity and confidentiality- Entities collecting or processing data have a responsibility to ensure that reasonable steps have been taken to implement security safeguards. This includes ascertaining the integrity of all employees authorised to access an individual's personal information.

(vii) Accountability – Entities collecting and/or processing data must ensure that their practices are compliant with the other principles.

The processing , of any personal data – meaning the collection, storing or usage, exposes data subjects to risks of data being inadvertently released, stolen, used in activities that are contrary to the law or used for purposes unknown to the data subject.

A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. A DPIA may not eliminate such risks altogether but should help to identify and manage them. There is often more than one way of designing a project.

A DPIA can help identify the least privacy intrusive way of achieving a legitimate aim. Programs and activities relating to the processing of personal data must comply with legal and policy requirements. The Act recognises the need for data controllers and data processors to implement appropriate technical and organisational measures to minimize negative impacts on the privacy of data subjects. This requirement is detailed in section 41 which provides that data controllers and data processors have a duty to implement data protection principles in an effective manner; integrate necessary safeguards into the processing; and ensure that only personal data necessary for each specific purpose is processed. The adoption of this provision ensures that all data controller and processors are designing all processing activities to ensure data protection by design and/or default.

DPIAs are an early warning system, allowing institutions to identify and mitigate risks as early and as completely as possible. They are a key tool for decision-makers, enabling them to deal with issues internally and proactively rather than waiting for complaints, external intervention, investigations and bad press, amongst other things.

7. PURPOSE OF GUIDELINES

The Guidelines were developed to assist data controllers and data processers understand their obligations under the Act and appreciate the need to undertake a Data Protection Impact Assessment. Further, the guidelines aim to assist data controllers and data processors understand the risks of any processing activities undertaken and know when a Data Protection Impact Assessment is to be carried out and submitted to the Office pursuant to the provisions of the Act.

8. SCOPE OF GUIDELINES

The Act provides for the carrying out of a Data Protection Impact Assessment (DPIA). Further, the Act gives the Office of the Data Protection Commissioner the mandate to set out Guidelines for the carrying out of the Data Protection Impact Assessment (Section 31(6)).

A Data Protection Impact Assessment (DPIA) is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of a data subject resulting from the processing of personal data (as defined in the Act) by assessing them and determining the measures to address them. The purpose of a DPIA is to demonstrate the implementation of the data protection principles to ensure that data subjects retain control over their personal data. Additionally, DPIAs are important tools for:

- negating risk;
- accountability;
- identifying the impacts an entities activities/ programs will have on a data subject's right to privacy;
- providing input to design for privacy protection (necessary to meet privacy by design/ default obligations)
- Demonstrate that appropriate measures have been taken to ensure compliance with the provisions of the Act.

The Act, in Section 31, states that a data privacy impact assessment is needed *"where a processing operation is likely to result in a high risk to the rights and freedoms of a data Subject, by virtue of its nature, context, scope or purpose".*
The Data Protection Act does not formally define the concept of a DPIA as such, but - its minimal content is specified in Section 31(2) as follows:

*"**(a)** a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor;*
***(b)** an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
***(c)** an assessment of the risks to the rights and freedoms of data subjects."*

These Guidelines take account of:

- The Act;
- The Data Protection and Privacy Policy; and
- International standards.

The Act does not provide for a mandatory carrying out of a DPIA by all data controllers and data processors. However, a DPIA is a pre-requisite when the processing of personal data is "likely to result in a high risk to the rights and freedoms of data subjects" (Section 31).

9. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The obligation for data controllers and data processors to conduct a DPIA in certain circumstances must be understood against the background of their duty to implement appropriate technical and organisational measures to appropriately manage risks presented by the processing of personal data. In order to manage the risks to the rights of data subjects, the data controllers and data processors must have an understanding of the processing activity to be undertaken, ensure that appropriate measures have been implemented and safeguards integrated and the risk posed must be identified, analysed, estimated, evaluated, treated and reviewed regularly.

A "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. Section 31 refers to a likely high risk "to the rights and freedoms of data subjects". The reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights as enumerated in Chapter Four of the Constitution of Kenya 2010.

The fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish data controllers' or data processors' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. In practice, this means that data controllers and data processors must continuously assess the risks created by their processing activities in order to identify when a type of processing is "likely to result in a high risk to the rights and freedoms of data subjects".

A. Which processing operations are subject to a DPIA?

The carrying out of a DPIA is only mandatory where processing is "likely to result in a high risk to the rights and freedoms of data subjects". In cases where it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers and/or data processors comply with data protection law. In addition to the aforesaid, the Act requires that all data controller and processers implement appropriate technical and organisational measures

and integrate appropriate safeguards to ensure the adequate protection of personal data of data subjects.

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Section 31(1) and other provisions of the Act, the following nine criteria should be considered.

I. **Automated-decision making with legal or similar significant effect:** processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Section 35). This includes profiling and predicting, especially from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

II. **Systematic monitoring:** processing used to observe, monitor or control data subjects, including data collected through networks or public surveillance equipment. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).

III. **Sensitive personal data or data relating to a data subject or matters of a private nature:** this includes special categories of personal data as defined in Section 2. The Act provides for categories of data that can be considered as increasing the possible risk to the rights and freedoms of data subject and defined these classes as "sensitive personal data".

IV. **Data processed on a large volumes or large scales:** The Act does not define what constitutes large volumes or scales. The following factors are to be considered when determining whether the processing is carried out on a large scale:
(a) The number of data subjects concerned;
(b) The volume of data and/or the range of different data items being processed;

(c) The duration, or permanence, of the data processing activity;
(d) The geographical extent of the processing activity.

V. **Matching or combining datasets:** personal data originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

VI. **Data concerning vulnerable data subjects:** the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller and/or data processor, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees, more vulnerable segments of the population requiring special protection (minorities, persons with disabilities , asylum seekers and refugees, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the data controller and/or data protector can be identified.

VII. **Innovative use or applying new technological or organisational solutions:** Technology can involve novel forms of data collection and usage, possibly with a high risk to data subjects' rights and freedoms. The personal and social consequences of the deployment of a new technology may be unknown; however, a DPIA will help the data controller and/or data processor to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore, require a DPIA.

VIII. When the processing in itself prevents data subjects from exercising a right. This includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract.

A processing operation may fall within the above-mentioned criteria and still be considered by the data controller or data processor not to be "likely to result in a high risk". In such cases the data controller and data processor

must seek concurrence from the Office or the Data Protection Commissioner and should justify the reasons the data controller and/ or data processor does not believe a DPIA is necessary.

B. <u>When should a DPIA be submitted?</u>

Pursuant to the Act, a DPIA must be submitted 60 days prior to the commencement of the processing of personal data. However, given that the Act has come into place at a time where data controllers and data processors have commenced processing activities of the kind envisaged under the Act, the Office recommends that those processing data that is "likely to result in a high risk" to rights of data subjects, submit DPIA, as this would be taken into consideration in the event of a breach, or other factor likely to attract an administrative fine/penalty.

C. <u>When is a DPIA required?</u>

The Act does not prescribe whether a DPIA may concern a single data processing operation or whether a single DPIA could be used to access multiple, similar, processing operations. These guidelines, in adoption of international standards and practices, allow for the use of a single assessment to address a set of similar processing operations that present similar high risks. These guidelines acknowledge that there are circumstances under which it may be reasonable and economical for the subject of a DPIA to be broader than a single project or activity. A similar data processing operation is one where the nature, scope, context, purpose and risk are similar to a previous data processing operation for which a DPIA has been conducted.

In light of the above, a DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. If the processing operation involves joint data controllers and/or data processors the DPIA needs to define the respective obligations of all parties involved in the processing precisely. A joint DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller and/or data processors should express its needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential).

Any data processing whose conditions of implementation (scope, purpose, personal data collected, identity of the data controllers or recipients, data

retention period, technical and organisational measures, etc.) have changed since the initial approval by the Office of the Data Protection Commissioner and which are likely to result in a high risk should be subject to a DPIA.

A DPIA is required after a change of the risks resulting from the processing operations, for example because a new technology has come into use or because personal data is being used for a different purpose. The revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over time. A DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, or new categories of data subjects become vulnerable to discrimination.

D. When is a DPIA not Required?

The Act provides that a DPIA is required when processing is "likely to result in a high risk". Therefore, it follows that when processing is not likely to result in a high risk, that a DPIA does not need be carried out. However, a data controller or data processor must comply with the other provision of the Act, including but not limited to section 41.

A DPIA is not required in the following cases:

- where the processing is not "likely to result in a high risk to the rights and freedoms of data subjects";

- when the nature, scope, context, purpose and risk of the processing are very similar to the processing for which DPIA have been carried out. In such cases, results of DPIA for similar processing can be used; and

- where processing falls under the exceptions under section 51(2).

E. How to carry out a DPIA?

The Act in Section 31(3) provides that a DPIA should be carried out by a data controller and/or data processor *"prior to the processing if a data protection impact assessment prepared under this section indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject".* This is consistent with data protection by design and by default principles articulated in Section 41 and 42 of the Act.

The DPIA should be started as early as is practicable in the design of the

processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organisational measures may affect the severity or likelihood of the risks posed by the processing.

The fact that the DPIA may need to be updated once the processing has actually started is not a valid reason for postponing or not carrying out a DPIA. The DPIA is an on-going process, especially where a processing operation is dynamic and subject to ongoing change.

The Act sets out the minimum requirements of a DPIA (Section 31(1). However, guidance is also given in Sections 41 and 42 as to matters need to be addressed in a DPIA. The following matters must be addressed in a DPIA:

(i) the amount of personal data collected;
(ii) the extent of processing of the personal data;
(iii) the period and method of storage of the personal data and its accessibility;
(iv) the state of technological development available for processing;
(v) the special risks that exist in the processing of the data;
(vi) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor;
(vii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(viii) an assessment of the risks to the rights and freedoms of data subjects; and
(ix) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights, and legitimate interests of data subjects and other persons concerned (section 31(1)(d).

OFFICE OF THE DATA PROTECTION COMMISSION
DATA PROTECTION IMPACT ASSESSMENT

Instructions

1. Fill out this template prior to the commencement of any processing activity of personal data, or if you are making a significant change to an existing process.

2. Integrate the final outcomes back into your project plan.

Part 1: Description of the processing operations

1.	Project Name	
2.	Project Outline: What and why Explain broadly what the project aims to achieve and what type of processing it involves	
3. a. b.	Who are the targeted data subjects? What is the classes of data are to be collected; What is the class of data subjects (i.e. are there any vulnerable groups/ children that form part of the data subjects)	
4.	Describe the Information Flow Describe the collection, use and deletion of personal data here. It may in a flow diagram or another format of explaining data flows	
a) b) c) d)	where you are getting the data from; how is the data being collected; how much data is likely to be collected; where the data will be stored;	

e) f) g) h)	How long will the data be stored; To what extent is the data being processed where data could be transferred to; and how many individuals are likely to be affected by the project.	
5. a. b. c. d. e. f. g.	Describe how the data processing flow complies with the seven data protection principles- Lawfulness, fairness and transparency Purpose limitation Data minimisation Accuracy. Storage Limitation Integrity and confidentiality Accountability	

Part 2: An assessment of the necessity and proportionality of the processing operations in relation to the purpose.

Describe compliance & proportionality, measures, in particular:		
1.	What is your lawful basis for processing?	
2.	How is consent to be obtained, if at all?	
3.	Does the processing actually achieve your purpose?	
4.	Is there another way to achieve the same outcome?	
5.	How will you ensure data quality and data minimization?	

6.	What information will you give individuals?	
7.	How will you help to support their rights?	
8.	What measures do you take to ensure compliance by the Controller and Processor?	
9.	What parties are involved in the processing and what are their specific roles?	
10.	How do you safeguard the processing of the personal data?	
11.	How do you safeguard any international transfers?	

Part 3: An assessment of the risks to the rights and freedoms of data subjects.

ASSESSMENT QUESTIONS

Explain what practical steps you will take to ensure that you identify and address privacy risks.	**Yes. (Please Give explanation)**	**No. (Please Give explanation)**
1. Will the project involve the collection of new identifiable or potentially identifiable data about data subjects?		
2. Will the project compel data subjects to provide information about themselves, i.e., where they will have little awareness or choice? **3.** Will identifiable information about the data subjects be shared with other organizations or people who have not previously had routine access to the information?		

4. Are you using information about data subjects for a purpose it is not currently used for in a new way, i.e. using data collected to provide care for an evaluation of service development.		
5. Where information about data subjects is being used, would this be likely to raise privacy concerns or expectations, i.e. will it include health records, criminal records or other information that people may consider to be sensitive and private and may cause them concern or distress?		
6. Will the project require you to contact data subjects in ways, which they may find intrusive, such as telephoning or emailing them without their prior consent?		
7. Will the project result in you making decisions in ways which can have a significant impact on data subjects, i.e. will it affect the services a person receives?		
8. Does the project involve you using new technology which might be perceived as being privacy intrusive, i.e. using biometrics, facial recognition or automated decision making?		
9. Is a service being transferred to a new supplier (re-contracted) and the end of an existing contract?		
10. Is processing of identifiable / potentially identifiable data being moved to a new organization (but with same staff and processes)		

Part 4: The measures envisaged addressing the risks and the safe guards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Data Protection Act

Risk Assessment - Identifying Privacy Risks and Evaluating Privacy Solutions									
	Name of Data Controller/Processor /Project:_XXXX								Risk Register Owner: XXXX
Risk ID	Risk Description	Consequence	Risk Owner		Current internal CONTROLS (provide details of how you currently manage the risk)	Assessment of Risk			Describe what further ACTIONS you will take to reduce the Impact/Likelihood and mitigate the risk. State who is the risk owner for each action
						Impact (1,2,3,4,5)	Likelihood (1,2,3,4,5)	Score	

Part 5: Sign Off and Record Outcomes

ITEM DESCRIPTION	OFFICER NAME/DATE	NOTES/INSTRUCTIONS
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:		If accepting any residual high risk, consult the ODPP before going ahead
DPO advice provided:		DPO should advise on compliance, PART 4 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
Consultation with Office of the Data Protection Commissioner Response		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

OFFICE OF THE DATA PROTECTION COMMISSIONER

P.O. BOX 30920-00100

NAIROBI

info@odpc.go.ke | www.odpc.go.ke