REPUBLIC OF KENYA

OFFICE O F THE DATA PROTECTION COMMISSIONER

PERSONAL DATA PROTECTION HANDBOOK

Let's empower all stakeholders,
To protect personal data like treasure,
And spread light of responsibility, beyond measure.
Let's do this.

~

Immaculate Kassait

Table of Contents

About this Handbook.

The collection, use, and sharing of personal information has become an integral part of man's daily life. However, the increased use of personal data has also raised concerns about its protection and misuse. Personal data protection helps foster consumer trust and increases the use of digital tools, which can incentivize investment, competition and innovation in the digital economy. Several countries across the globe have developed and implemented personal data protection legislation to regulate the processing of personal data.

In Kenya, the right to privacy is enshrined in the Constitution, under Article 31 and subsequently, enactment of the Data Protection Act, 2019, which paved the way to the establishment of the Office of Data Commissioner in November, 2020 *to regulate the processing of personal data; ensuring that the processing of personal data of a data subject is guided by the principles set out in section 25 of the Act; protecting the privacy of individuals; establishing the legal and institutional mechanism to protect personal data; providing data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act.*

The Office of Data Protection Commissioner is an Independent State Office under the Ministry of Information, Communications and the Digital Economy. Further, the Government actualized the Data Protection Act, 2019 through development and publication of three sets of Data Protection Regulations and fully operationalized the Office.

This handbook has been designed to provide simplified information to Data Controllers and Data Processors who have the responsibility and obligation to uphold the principles of data protection. In addition, the handbook acts as an awareness wallet for data subjects to better understand their rights and available legal and institutional framework to protect their personal data from processing that is not covered under the existing personal data laws.

The handbook highlights legal and institutional mechanism on data protection in Kenya; Key Principles of data protection; defines personal data and types of personal data; explains who are data subjects, data controllers and data processors; gives practical advice on how to comply with personal data protection laws, including registration, reporting of complaints and personal data breach.

I am confident that this handbook will be a valuable resource for data controllers, data processors and data subjects as we walk together on the journey of safeguarding the privacy of Kenyans, as well as promoting the digital economy and the sovereignty of our beloved country.

I now invite you to read the handbook and look forward to an informed and empowered citizenry.

Immaculate Kassait, MBS

Data Commissioner,
Office of the Data Protection Commissioner.

Immaculate Kassait, MBS

Introduction to Personal data protection

Personal Data protection in Kenya is governed by the Data Protection Act of 2019. The Act gives effect to Article 31(c) and (d) of the Constitution of Kenya that contains the right to privacy which is a fundamental human right. provides for the protection of personal data by requiring organisations to obtain consent from individuals before collecting, using, or disclosing their personal information.

The Office of the Data Commissioner is responsible for ensuring compliance with data protection laws in Kenya. Individuals have a right to secrecy and privacy of their personal data. These data rights include the right to access, correct, and delete their personal information.

It is important for organizations in Kenya to be aware of and comply with the Data Protection Act in order to protect the personal information of individuals and to avoid potential penalties for non-compliance.

It is also important for individuals to be mindful of their own personal data privacy and to take steps to protect their information, such as reading privacy policies and being cautious about sharing personal information online.

Why Personal data protection is important.

Data privacy is crucial to protecting personal information, maintaining individual rights and preventing potential harm. It is an important aspect of building trust and maintaining positive relationships with individuals and other stakeholders.

Failing to protect personal information can have serious consequences:

- It can lead to identity theft.
- It can lead to financial fraud and other forms of abuse.
- It can damage an individual's reputation, and result in a loss of trust and confidence in an organization.

Organizations have legal and ethical obligations to protect personal data.

Principles of Personal Data Protection.

1.

Lawfulness, Fairness and Transparency:

Personal data must be processed lawfully, fairly and in a transparent manner.

2.

Purpose Limitation:

Personal data must be collected and processed for specified, explicit and legitimate purposes.

3.

Data Minimization:

Personal data should be limited to what is necessary for the specified, explicit and legitimate purposes.

4.

Accuracy :

Personal data should be accurate and, where necessary, kept up to date.

5.

Storage Limitation:

Personal data should be stored for no longer than is necessary for the specified, explicit and legitimate purposes.

6.

Accountability and Transparency:

The principle of accountability requires organizations to take responsibility for personal data and ensure individuals can exercise their rights, while transparency obligates organizations to provide clear information on data processing. Together, they ensure responsible data protection and understanding of data use.

7.

Integrity and Confidentiality:

Personal data should be secured and protected against unauthorized or unlawful processing and against accidental loss, destruction or damage.

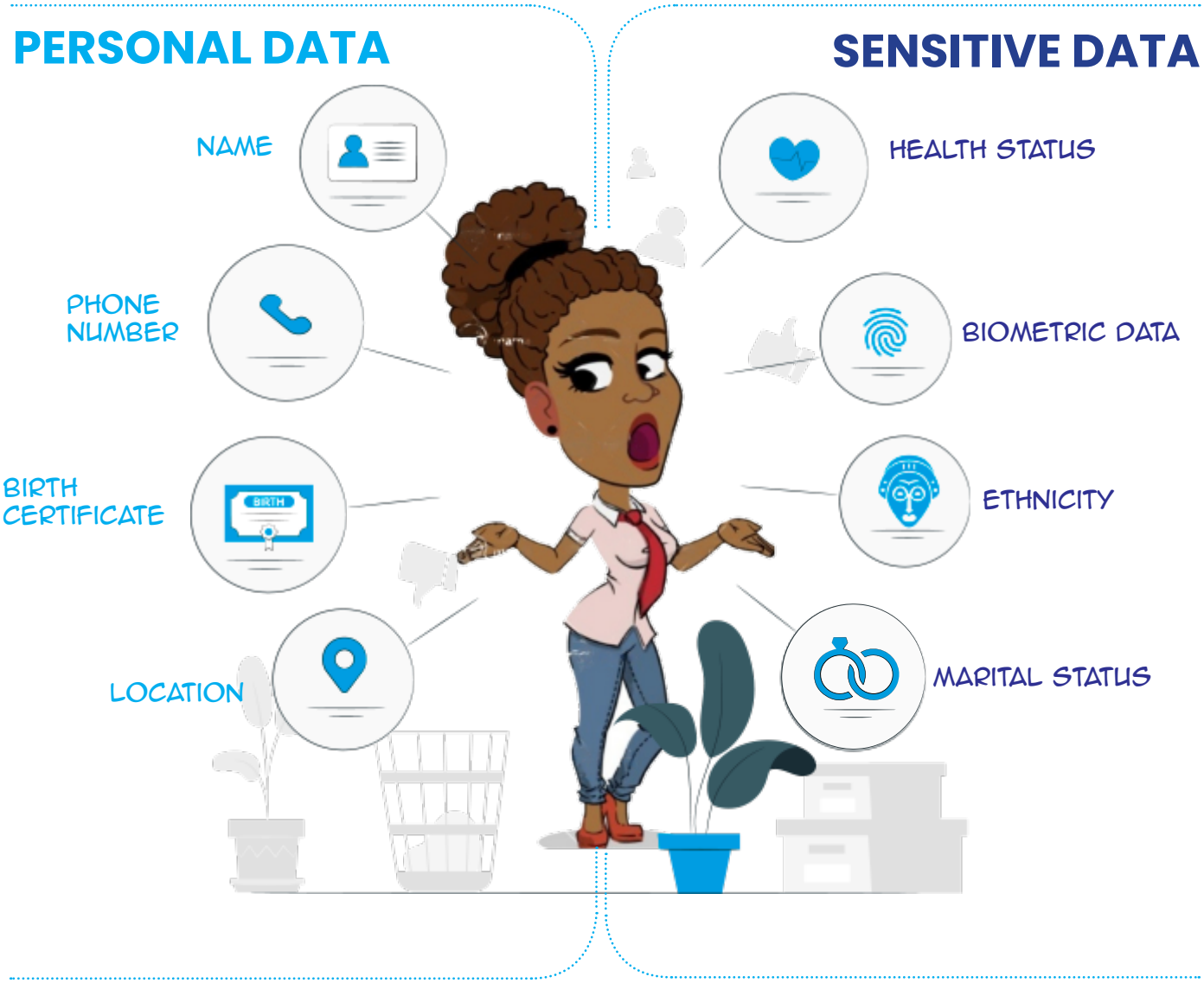
What is personal data?

Personal data is defined as any information that can be used to identify a natural person or any information that has the capability of identifying a natural person.

What is sensitive personal data?

Sensitive personal data is information that is very private and needs to be protected extra carefully under the law.

It's important to handle this kind of information with extra care to make sure it stays private and secure.



Note : These are a few common examples

Data subjects

Data subject is you and me. This is an identified or identifiable natural person who is the subject of personal data.

Ways that people give out their data

When making payment

When there is a need to access services both from government and private institutions i.e schools, hospitals etc

Accessing buildings

Signing up for online services or accounts

Filling out online

Using social media

Online shopping

Using digital apps

Who's a Data Controller / Data Processor?

In the context of personal data protection, Data Controllers are entities that determine the purposes and means of processing personal data, while Data Processors are entities that process personal data on behalf of data controllers.

Data Controller Examples

A bank collecting personal information from customers to open new accounts

A retail company collecting personal information from customers to send marketing emails

A hospital collecting personal information from patients for medical treatment

A government agency collecting personal information from citizens for tax purposes

A credit bureau collecting personal information from financial institutions for credit scoring

Data Processor Examples

A cloud storage provider storing personal information for a bank

A marketing agency sending emails to customers on behalf of a retail company

A billing and coding service processing medical claims for a hospital

A tax preparation software provider processing tax returns for a government agency

A collection agency collecting delinquent accounts on behalf of a credit bureau

Data subject rights including exercise of rights by minors

(a) To be informed of the use to which their personal data is to be put

(b) To access their personal data in custody of data controller or data processor

(c) To object to the processing of all or part of their personal data

(d) To correction of false or misleading data

(e) To deletion of false or misleading data about them

(f) Right to erasure

(g) Right to data portability

(h) Automated decision making

What is Personal Data Protection Compliance?

Data controllers can take the following steps to ensure compliance:

- **Register** as a data controller or data processor with the Office of the Data Protection Commissioner.
- **Renew** the certificate upon expiry.
- **Appointing** a personal data protection officer (optional).
- **Implement** data protection principles and ensure compliance throughout processing operations.(Section 25)
- **Ensure** that the processing of personal data is carried out lawfully.(Section 30)
- **Carry out** data protection impact assessments where the processing of personal data is likely to result in a high risk to the rights and freedoms of the data subject.
- **Implement** appropriate technical and organizational measures into processing operations to protect personal data from unauthorized access, disclosure, or destruction.
- **Report data breaches** to the data commissioner within 72 hours of becoming aware of them (data processors must report to data controllers within 48 hours).
- **Ensure appropriate safeguards** are in place for the transfer of personal data outside Kenya.
- **Meet localization requirements** by processing personal data through a data center located in Kenya or by storing a serving copy of the personal data in Kenya.
- **Develop policies** on data retention and data protection as required under the General Regulations.
- **Govern** regular sharing of personal data with a data sharing agreement.
- **Review** processing operations in relation to regulatory requirements to ensure compliance.

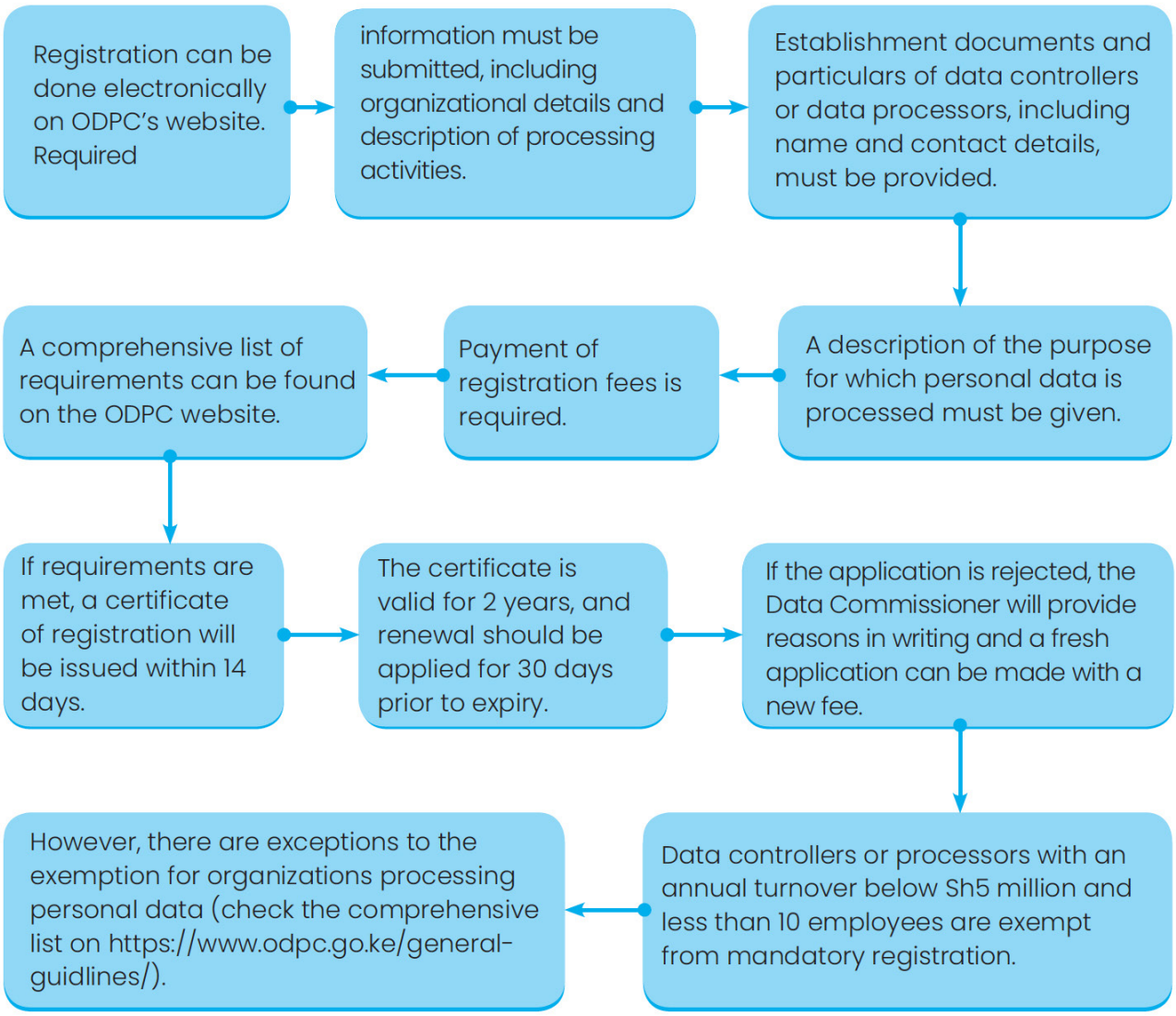
Processing sensitive personal data means handling private information about a person that could cause harm if it got into the wrong hands. Data controllers and processors need to follow rules to keep this information safe. They can only process sensitive personal data if there's a good reason, such as:

- It is part of a legitimate activity
- The person (data subject) has made the information public themselves.
- It is necessary for protecting someone's rights or interests.
- It is necessary for legal reasons, such as defending a legal claim.
- It is necessary for protecting the vital interests of the person.

Why Register with ODPC?

- Registration with the ODPC and compliance with the Data Protection Act helps build trust and confidence in an organization.
- It helps prevent negative publicity and protect an organization's brand image.
- It helps improve data management practices and ensures that personal data is accurate and up-to-date.
- It help organizations to stay ahead of evolving data protection laws and regulatory requirements.
- It is a legal requirement under the Data Protection Act, 2019.

What is the process for registration?



Registration Fees:

The registration fee depends on the category of the data controller (DC) or data processor (DP), which is determined by their annual turnover/revenue and number of employees.
There are three categories: micro/small, medium, and large:

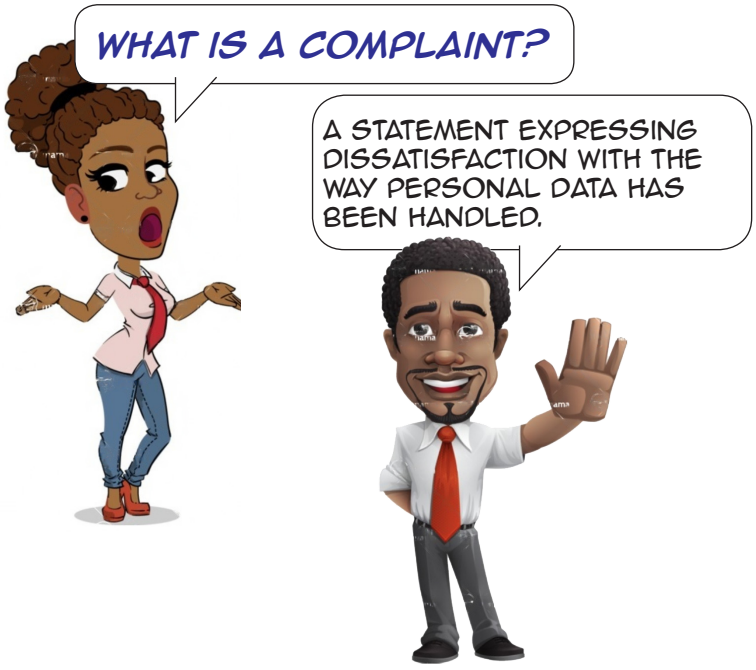
Category	Description	Registration Fee per DC or DP (Payable once)	Renewal fee per DC or DP (After every 2 years.
Micro and small data controllers/ processors	A data controller/processor with between 1 and 50 employees and an annual turnover/ revenue of a maximum of Sh5 million.	**Sh. 4,000**	**Sh. 2,000**
Medium data controllers/ processors	A data controller/processor with between 51 and 99 employees and an annual turnover/ revenue of between Sh5,000,001 and maximum of Sh50,000,000	**Sh. 16,000**	**Sh. 9,000**
Large data controllers/ processors	Data controller/processor with more than 99 employees and an annual turnover/revenue of more than Kes 50 Million	**Sh. 40,000**	**Sh. 25,000**
Public entities	Data controller/processor offering government functions (regardless of number of employees or revenue/ turnover)	**Sh. 4,000**	**Sh. 2,000**
Charities and religious entities	Data controller or processor offering charity or religious functions (regardless of revenue/ turnover).	**Sh. 4,000**	**Sh. 2,000**

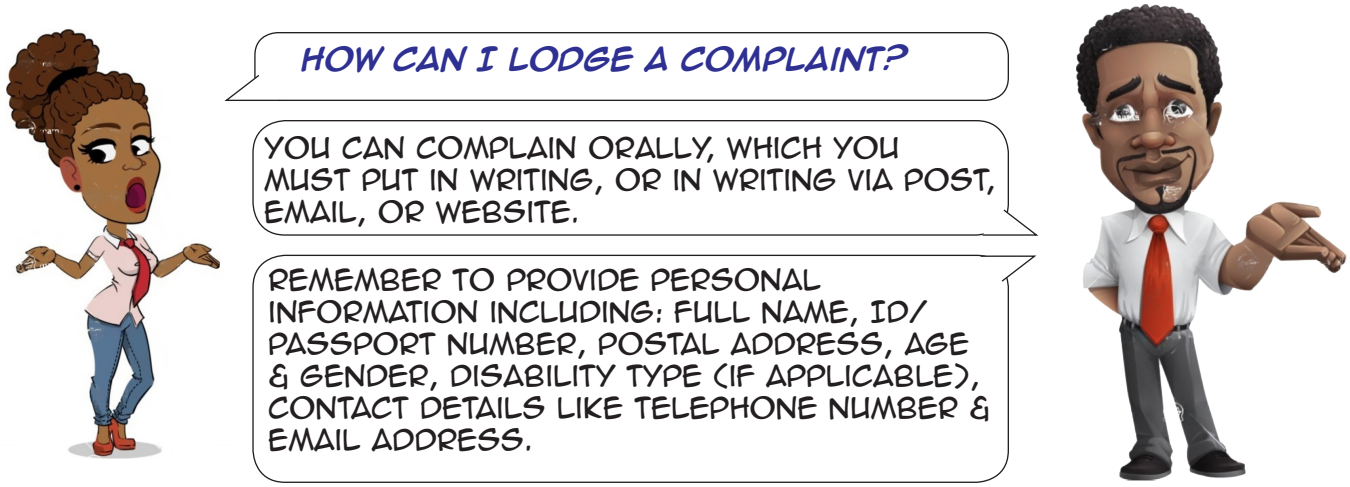
Additional Information on Registration:

- All public and non-profit entities must register regardless of revenue. Civil Registration Entities are exempt.
- Applications are reviewed after payment confirmation, which may be delayed if payment is made by cheque.
- Data Controllers and Processors are to notify ODPC in writing within 14 days of any changes to the application.
- Certificate of registration is issued within 14 days after payment and provision of required information.
- Having a data protection officer is not mandatory, but recommended.

Complaints:

- A complaint is a statement expressing dissatisfaction with the way personal data has been handled.
- A complainant is a person who has lodged a complaint with the Office of Data Protection Commissioner (ODPC).
- Who can complain?
  - »The complainant in person
  - »A person acting on behalf of the complainant
  - »Any other person authorized by law to act on behalf of a data subject
  - »Or anonymously.





How to lodge a complaint:

- Complain orally (which must be put in writing) or in writing via post, email, or website.
- Provide personal information including:
  - »Full name
  - »ID/passport number
  - »Postal address
  - »Age & Gender
  - »Disability type (if applicable)
  - »Contact details (telephone number & email address)
- Provide information about the respondent, including:
  - »Names and contact details of the respondent (institutional and individual)
  - »Date of occurrence of the alleged infringement
  - »Nature of the complaint
  - »Names of persons that can provide further information
  - »Particulars of any institution or person that has previously made any attempt to resolve the matter
  - »Any potential or actual harm or urgency, and any supporting documents.
- Anonymous complaints will be investigated to ascertain their veracity.
- Complaints will be acknowledged within 7 days of receipt.
- Complaints will be handled confidentially, and the Office will seek consent before disclosing any particulars.

Investigations

The Office conducts investigations on its own initiative or on the basis of a complaint made by a data subject.

Goals of investigations:
The goal of any investigation is to gather all relevant facts concerning a specific incident and determine the following:

- What happened?
- When did it happen?
- Where did it happen?
- Who was responsible?
- Who may have been affected?
- What further actions may be needed to prevent the alleged wrongdoing from recurring?

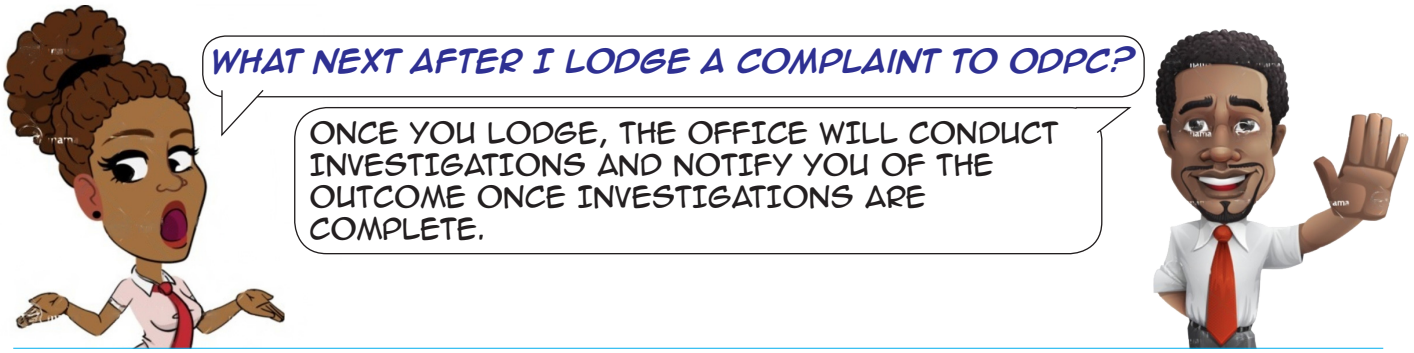
Investigation powers of the Office:

For the purpose of the investigation of a complaint, the Office of the Data Protection Commissioner may order any person to:

- Attend at a specified time and place for the purpose of being examined orally in relation to the complaint.
- Produce such book, document, record, or article as may be required with respect to any matter relevant to the investigation.
- Furnish a statement in writing

Investigation timeline:

- A complaint made to the Office of the Data Protection Commissioner shall be investigated and concluded within ninety (90) days.



Enforcement

Enforcement action:

On the completion of an investigation, any corrective action, if necessary, will be promptly taken by the issuance an Enforcement Notice or a Penalty Notice.

- An Enforcement Notice is issued to person or entity that has failed to comply with the provisions of the Data Protection Act, and it specifies the measures to be taken to remedy the situation, the consequences of failure to comply, and the period for compliance.
- The parties have the right to apply for a review of the Enforcement Notice to the ODPC and the right to appeal to the High Court.
- A Penalty Notice is issued to a person or entity that has failed to comply with an Enforcement Notice after the specified period, and it states the penalty to be paid.
- A Penalty Notice can be issued immediately upon satisfaction by theData Commissioner of a person's/entity's failure to comply or after the lapse of the enforcement notice period.
- The parties have the right to appeal against the Penalty Notice to the High Court.
- The penalty specified in the Penalty Notice is due immediately upon issuance, within the specified time period, on the final determination of any appeal, or on the lapse of the period given to appeal.

OFFICE OF THE DATA PROTECTION COMMISSIONER

Tel: +254752896867 | +254796954269
Office: 12th Floor, Britam Tower, Hospital Road, Upperhill.
Web: www.odpc.go.ke