DATA PROTECTION GUIDELINE

FOR MEMBERS OF THE INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS OF KENYA

MARCH 2026

Contents

1. Introduction to personal data protection 4
2. Scope and applicability 4
3. Importance of protection of personal Data 5
4. Key terms in data protection 5
4.1 What is personal data? 5
4.2 What is sensitive personal data? 5
4.3 Data Subjects 5
4.4 Filing System 6
4.5 Processing 6
5 Ways that people give out their data 6
6 Principles of personal Data protection 6
7 Legal Grounds for Processing personal sensitive data in Finance and Accounting 7
8 Consent 8
9 Rights of Data Subjects in Accounting Setting 9
10. Use of Automated Tools in accountancy (ERP, AI Accounting) 9
11. Personal data protection Compliance 10
12. Reason for registration with the Office of the Data Protection Commissioner (ODPC) 11
Registration fees: 12
Important information on registration 13
13. Data governance 13
13.1 Appointment of a Data Protection Officer (DPO) 13
13.2 Data Protection Impact Assessments (DPIAs) in accounting 14
13.3 Retention and Disposal of Accounting Data 14
13.4 Cross-Border Data Storage (Cloud Accounting Tools) 15
13.5 Data Security Measures 15
14. Complaints 16
15. Investigations 17
16. Enforcement 18

DATA PROTECTION GUIDELINE

ABOUT THIS GUIDELINE

The Data Protection Guideline establishes the regulatory framework of data protection and data privacy for members of the Institute who are data processors or data controllers. It establishes the compliance requirements and operational needs while collecting or processing personal data.

This Guideline is developed to govern members of the Institute as they practice accountancy pursuant to section 2 of the Accountants Act no 15 of 2008 and in the process access, process or store personal data.

This guideline adheres to the Data Protection regulatory framework in Kenya and in particular Article 31 of the Constitution of Kenya, 2010 and the Data Protection Act, 2019 and its regulations.

Adherence to this guideline signifies commitment to compliance with the rights and obligations established under the Data Protection Act ,2019 for Data Controllers, Data Processors and Data Subjects.

The guideline highlights the procedures, controls and safety measures to be put in place by all stakeholders in the data protection matrix and mitigation measures set out in the Data protection Act, 2019 to ensure personal data is kept confidential and secure.

All members of the Institute are required to acquaint themselves with the contents of this guideline and to put in place procedures that ensure adherence to the Constitution of Kenya, 2010, the Data Protection Act, 2019 and its Regulations and all enabling legislation.

1. INTRODUCTION TO PERSONAL DATA PROTECTION

Personal Data protection in Kenya is regulated by the Data Protection Act of 2019(the Act). The Act gives effect to Article 31(c) and (d) of the Constitution of Kenya that established the right to privacy. The law provides for the protection of personal data by requiring organizations to obtain consent from individuals before collecting, processing, using, or disclosing their personal information.

The Act established the Office of the Data Commissioner and bestows it with the responsibility of ensuring compliance with data protection laws in Kenya. Individuals have a right to confidentiality and privacy of their personal data. These data rights include the right to access, amend, and erase their personal information.

It is important for members of the Institute to be aware of and comply with the Data Protection Act in order to protect the personal information of individuals they interact with and to avoid potential consequences for non-compliance.

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

This guide is designed to help accountants comply with the requirements of the Act by:

i. Understanding the exact legal obligations imposed under the Act.

ii. Applying data protection principles in accounting, auditing, and finance.

iii. Recognizing data protection risks within accounting functions.

iv. Aligning their conduct with the expectations outlined in the Data protection Act, 2019 and other regulatory guidelines.

Accountant must incorporate data protection into their professional conduct and ensure that personal data is processed lawfully, fairly, and in a transparent manner.

2. SCOPE AND APPLICABILITY

The Act applies to any person who processes personal data and is established or ordinarily resident in Kenya and processes personal data while in Kenya or not established or resident in Kenya, but processes personal data of data subjects located in Kenya.

This guide is applicable to:

i. Public and private sector accountants.

ii. Certified Public Accountants (CPAs) and tax agents.

iii. Audit firms, payroll service providers, and finance teams.

iv. Accountants who process data on behalf of clients or employers.

3. IMPORTANCE OF PROTECTION OF PERSONAL DATA

Data privacy is necessary to protect personal information from potential harm and misuse and to safeguard individual rights. It is an important aspect of building trust and maintaining positive relationships between members of the Institute and other stakeholders.

Failing to protect personal information can have serious consequences:

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

Members of the Institute have legal and ethical obligations to protect their personal data and that of their stakeholders.

4. KEY TERMS IN DATA PROTECTION

4.1 What is personal data?

Personal data is any information that can be used to identify a natural person. Examples of personal data include names, telephone numbers, birth certificates and location.

4.2 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 is information that has a high potential for discrimination or abuse and therefore requires an extra level of protection. Examples of sensitive personal data include the health status of an individual, biometric data, ethnicity and marital status.

4.3 Data Subjects

A data subject is an identified or identifiable natural person who is the subject or focus of personal data. It is you and me.

4.4 Filing System

Filing system means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

4.5 Processing

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.

4.6 Data Controller or Data Processor

Data Controllers are establishments that determine the purposes and means of processing personal data for example the Institute collecting personal information from members to include them in the membership register, while Data Processors are entities that process personal data on behalf of data controllers for example a tax preparation software provider for an accountancy firm.

5 Ways that people give out their data

People give out their data –

i. When making payments
ii. When accessing services
iii. When accessing buildings
iv. When signing up for online services or accounts
v. When using social media
vi. When shopping online
vii. When using digital apps

6 Principles of personal Data protection

i. **Lawfulness, fairness and transparency**: personal data must be processed in a lawful, fair and transparent manner. Accountants should ensure that data

is collected and processed lawfully, fairly, and in a transparent manner in relation to the data subject.

ii. **Purpose limitation**: personal data must be accessed, processed and collected for a specified, explicit and legitimate purpose.

iii. **Data minimization**: Members of the Institute shall collect only the personal data that is necessary for the intended purpose and shall avoid excessive or irrelevant data collection.

iv. **Accuracy**: Reasonable steps should be taken to ensure that personal Data is accurate complete and periodically updated. Measures should be put in place to allow for the rectification of inaccurate or incomplete data in good time.

v. **Storage limitation:** Members of the institute are urged not to retain personal data for longer than it is necessary and for the sole reason for which the data was collected and stored unless obligated by law or legitimate requirements.

vi. **Accountability and transparency**: members of the Institute shall take responsibility for personal data and ensure that third parties can exercise their rights clearly and transparently.

vii. **Integrity and confidentiality:** Members of the Institute shall put in place safety measures to guard personal data from unauthorized access, editing, exposure, damage, or loss.

viii. **Transfer of Personal Data Outside Kenya:** The data controller or data processor shall ensure personal data is not transferred outside Kenya, unless there is a proof of adequate data protection safeguards or consent from the data subject. Accountants, especially those in managerial or audit roles, must document and demonstrate compliance with these principles.

7 Legal Grounds for Processing personal sensitive data in Finance and Accounting

Under the Data Protection Act, 2019, personal data must be processed on a lawful basis. This is outlined in Section 30 of the Act and accountants must ensure that every processing activity aligns with one of the lawful bases including:

i. **Consent**

Processing of personal data shall be lawful if the data subject has given consent to the processing for one or more specified purposes. In practice,

accountants might request consent to store client financial records or share them with third-party tax consultants.

ii. Contractual Necessity

Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

iii. Legal Obligation

Processing is necessary for compliance with a legal obligation to which the controller is subject. This includes obligations such as tax reporting, statutory audits, or payroll compliance with the Kenya Revenue Authority or Retirement Benefits Authority.

iv. Vital Interests

Processing is necessary in order to protect the vital interests of the data subject or another natural person. Though rare in accounting, this might arise where immediate access to a data subject's financial details is necessary in emergency situations.

v. Public Interest or Official Authority

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

vi. Legitimate Interests

Processing is necessary for the purposes of the legitimate interests pursued by the data controller or data processor or by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject.

8 CONSENT

Accountants must obtain valid consent before processing personal data unless another lawful basis applies. The Act provides that a data subject shall have the right to withdraw their consent at any time.

When sharing financial or employment data with third parties (e.g., auditors, tax consultants, HR system vendors), accountants must first obtain the client's or employee's express consent unless the disclosure is required by law.

A data controller shall notify a data subject of the purposes for which the personal data is being collected, used or disclosed. Additionally, the Act requires that a data

controller or data processor shall ensure that it is as easy to withdraw consent as to give it.

9 RIGHTS OF DATA SUBJECTS IN ACCOUNTING SETTING

The Data Protection Act, 2019 establishes clear rights for all data subjects. These rights apply in full to personal data collected and processed by accountants.

i. **Right to Be Informed**
A data subject has a right to be informed of the use to which their personal data is to be put.

ii. **Right of Access**
To access their personal data in custody of data controller or data processor. Accountants must be able to retrieve and provide a copy of a data subject's personal data upon request.

iii. **Right to Object**
To object to the processing of all or part of their personal data.

iv. **Right to Correction**
To correction of false or misleading data. A data controller or data processor shall rectify without undue delay, personal data in its possession or under its control that is inaccurate, incomplete or misleading.

v. **Right to Deletion**
To deletion of false or misleading data about them.

vi. **Right to Data Portability**
A data subject may request to receive personal data concerning them in a structured, commonly used and machine-readable format. Where feasible, the data subject may request transmission of their personal data to another data controller.

vii. **Right Not to Be Subject to Automated Decision-Making**
A data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling which produces legal effects concerning or significantly affect the data subject. The data controller must implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

10. USE OF AUTOMATED TOOLS IN ACCOUNTANCY (ERP, AI ACCOUNTING)

With the rise of Enterprise Resource Planning (ERP) systems and AI-driven accounting tools, professionals in audit and finance must be aware of data protection obligations when deploying automated decision-making technologies.

The Act provides that every data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject.

This means that accountants and firms using automated tools, such as AI models to flag transactions, credit risk assessments, or audit scoring algorithms, must not solely rely on these systems to make decisions that impact data subjects significantly, unless an exception applies.

Exceptions under this provision are:

i. where the decision is necessary for entering into or performing a contract.

ii. where the decision is authorized by law; or

iii. where the data subject has given explicit consent.

Where such automated processing is used, the data controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, including the right to obtain human intervention.

11. PERSONAL DATA PROTECTION COMPLIANCE

Data Controllers can take the following steps to ensure compliance with data protection laws:

i. Register as a data controller or data processor with the Office of the Data Protection Commissioner
ii. Renew the certificate of registration upon expiry
iii. Appoint a data protection officer (optional)
iv. implement the data protection principles and ensure compliance throughout processing operations
v. Ensure the processing of personal data is carried out lawfully
vi. Carry out data protection impact assessment tests where the processing of personal data is likely to result in a high risk to the rights and freedoms of the data subject
vii. Implement appropriate technical and organizational measures into processing operations to protect personal data from unauthorized access, disclosure, or destruction

viii. Report data breaches to the data commissioner within seventy-two (72) hours of becoming aware of them while a data processor must report to the data controllers within forty-eight (48) hours
ix. Ensure appropriate safeguards are in place for the transfer of personal data outside Kenya
x. 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
xi. Develop policies on data retention and data protection as required under the Data Protection (General) Regulations, 2021.
xii. Govern regular sharing of personal data with a data sharing agreement
xiii. Review processing operations in relation to regulatory requirements to ensure compliance.

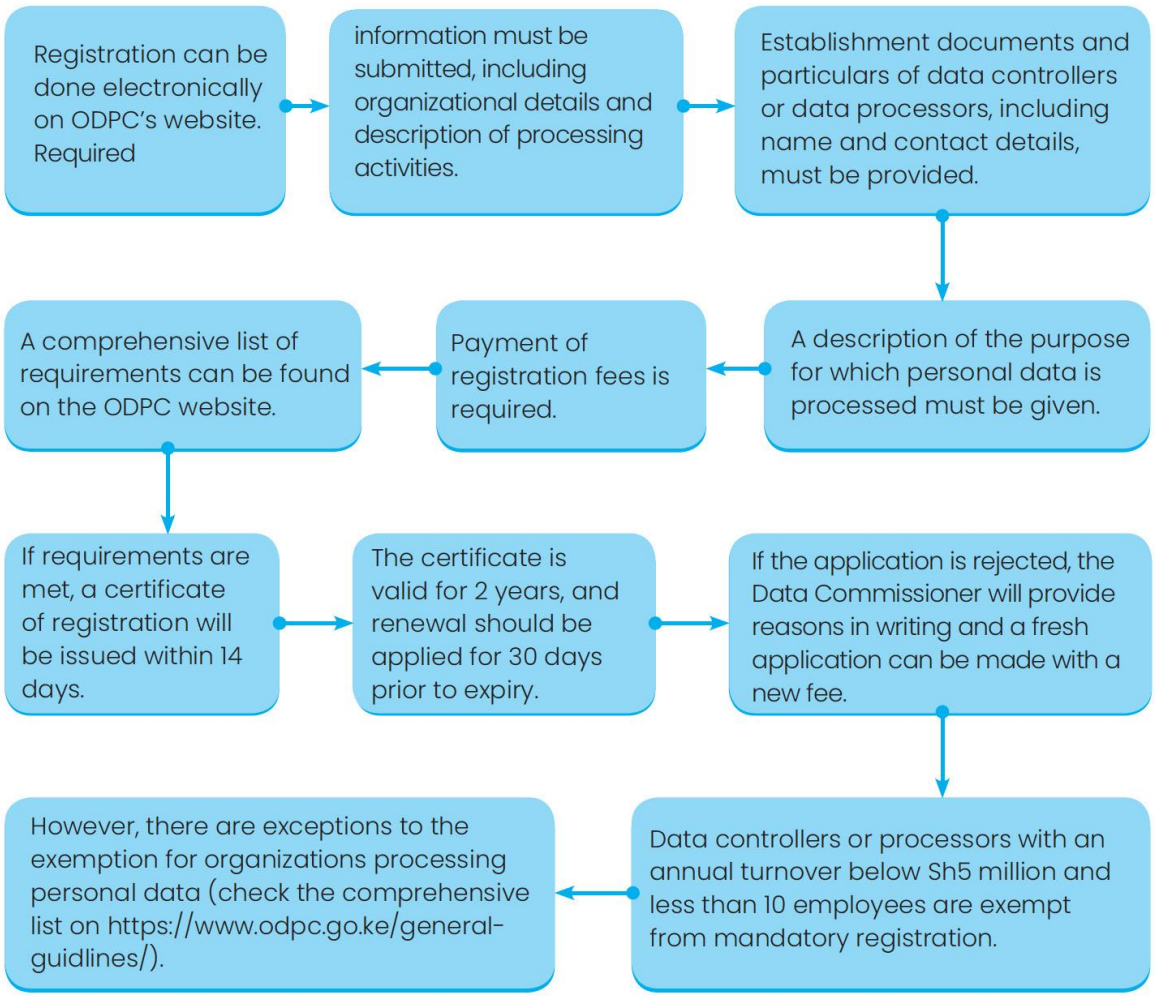
12. REASON FOR REGISTRATION WITH THE OFFICE OF THE DATA PROTECTION COMMISSIONER (ODPC)

Registration of Data Controllers and Data Processors with the ODPC It is a legal requirement under the Data Protection Act, 2019.

The benefits of registration include:

i. Registration with the ODPC and compliance with the Data Protection Act helps build trust and confidence in an organization.
ii. Registration helps prevent negative publicity and protect an organization's brand image.
iii. Registration improves data management practices and ensures that personal data is accurate and up-to-date.
iv. Registration helps organizations to stay ahead of evolving data protection laws and regulatory requirements.

The process of registration is as follows;



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**

Important information on registration

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

13. DATA GOVERNANCE

Data governance refers to frameworks, policies, roles, responsibilities, and processes that ensure accountability for data protection compliance. Accounting professionals and firms, as data controllers or processors, must establish clear governance mechanisms to ensure compliance with the Data Protection Act.

13.1 Appointment of a Data Protection Officer (DPO)

A data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine.

A DPO may be internal or external and is responsible for:

i. Advising the firm on compliance obligations.

ii. Monitoring adherence to data protection policies and procedures.

iii. Providing training for staff.

iv. Acting as a contact point for the ODPC and data subjects.

13.2 Data Protection Impact Assessments (DPIAs) in accounting

Accounting and audit professionals must conduct Data Protection Impact Assessments (DPIAs) when introducing new technology (e.g., cloud-based ERP, AI-based audit tools) or outsourcing functions that involve large-scale processing of personal data, such as payroll services or customer finance platforms.

According to the Data Protection Act, 2019, 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, scope, context and purposes, the data controller or data processor shall, prior to the processing, carry out a data protection impact assessment.

This means that if your firm is implementing new systems that process sensitive or high-volume personal data, a DPIA is legally required *before* rolling out the process or technology.

If the risks cannot be sufficiently mitigated, the data controller must consult with the Data Commissioner before processing.

13.3 Retention and Disposal of Accounting Data

A data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is—

i. required or authorised by law;

ii. reasonably necessary for a lawful purpose;

iii. authorised or consented to by the data subject; or

iv. or historical, statistical, journalistic, literature and art or research purposes.

13.4 Cross-Border Data Storage (Cloud Accounting Tools)

Many accountants and audit professionals in Kenya use international cloud-based platforms such as QuickBooks Online, Zoho Books, or Xero which often host personal data outside the country. This makes cross-border data transfer rules especially relevant for finance practitioners.

According to the Data Protection Act, 2019, A data controller or data processor may transfer personal data to another country only where the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data.

This means if you or your firm are using accounting software that stores data on foreign servers, you must ensure that appropriate safeguards are in place and demonstrable.

Examples of safeguards include:

i. Standard contractual clauses,

ii. Binding corporate rules, or

iii. Adequacy decisions where the receiving country is deemed to offer sufficient data protection standards.

13.5 Data Security Measures

Accountants and audit professionals frequently handle highly sensitive personal data, such as payroll, financial statements, tax records, and client information. A personal data breach in this context could include emailing the wrong client's payslip, exposing general ledger files on unsecured platforms, or unauthorized access to audit work papers.

13.5.1 Obligation to Notify the Data Commissioner

Where personal data has been accessed or acquired by an unauthorized person and there is a real risk of harm to the data subject, the data controller shall:

i. Notify the Data Commissioner without delay, and within seventy-two (72) hours of becoming aware of the breach.

ii. If the notification is not made within 72 hours, it must be accompanied by reasons for the delay.

13.5.2 Obligation to Notify the Data Subject

The data controller shall communicate to the data subject in writing within a reasonably practical period, unless:

i. The identity of the data subject cannot be established, or

ii. Communication is delayed or restricted for purposes of prevention, detection, or investigation of an offence by a relevant body.

13.5.3 Obligation of the Data Processor

If a data processor becomes aware of a personal data breach, they shall notify the data controller without delay, and where reasonably practicable, within forty-eight (48) hours of becoming aware of the breach.

13.5.4 Grounds for Delaying Notification to the Data Subject

The data controller may delay or restrict communication to the data subject if it is necessary and proportionate to enable the prevention, detection or investigation of an offence by a concerned authority.

13.5.5 Contents of Notification and Communication

The notification to the Data Commissioner and communication to the data subject shall include:

i. Description of the nature of the data breach.
ii. Measures taken or planned to address the breach.
iii. Recommendations for the data subject to mitigate adverse effects.
iv. Identity of the unauthorized person, if applicable.
v. Contact information of the Data Protection Officer or relevant contact point.

13.5.6 Exceptions to Communication with Data Subject

Communication of the breach to the data subject is not required where the data controller or processor has implemented appropriate security safeguards, such as encryption of the affected data.

If it is not possible to provide all the information at once, the data controller may provide the information in phases, but without undue delay.

13.5.7 Record-Keeping Requirement

The data controller shall maintain a record of the following in relation to each breach:

i. Facts relating to the breach.

ii. Effects of the breach.

iii. Remedial action taken.

14. Complaints

A complaint is a report expressing discontent with the way personal data has been handled, and a complainant is the individual who has lodged a complaint with the office of the Data Protection Commissioner.

14.1 Who can complain?

i. The Complainant in person;
ii. A person acting on behalf of or representing the complainant;
iii. Any person authorized by law to act on behalf of a Data Subject; or
iv. An anonymous person.

14.2 How to lodge a complaint:

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

15. INVESTIGATIONS

The ODPC carries out investigations on its own initiative and notifies the party of the outcome once the investigations are finalized.

The aim of any investigation into a complaint by the ODPC is to establish all relevant facts concerning a specific incident and determine the following facts:

i. The chronology of events?
ii. When the incident took place?
iii. Where the incident took place?
iv. Who was responsible?
v. Who may have been affected?
vi. What additional actions may be required to avert recurrence of the alleged wrongdoing ?

The ODPC may order any person to perform any of the following acts in the course of investigations:

i. Enter appearance at a specified time and place for the purpose of being examined orally in relation to the complaint.
ii. Produce documented information such as a book, document, record, or article as may be required with respect to any matter relevant to the investigation.
iii. Provide a statement in writing.

A complaint made to the ODPC shall be investigated and concluded within ninety (90) days.

16. ENFORCEMENT

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

An Enforcement Notice is handed out to a person or entity that has breached the provisions of the Data Protection Act, and it specifies the actions to be taken to remedy the situation, the consequences of failure to comply, and the timeline 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 on the other hand is issued by the Data Commissioner to a person or entity that has failed to comply with an Enforcement Notice after the specified timeline, and it states the penalty to be paid.

The penalty specified in the Penalty Notice is owed immediately upon issuance, within the specified time period, on the final determination of any appeal, or upon lapse of the period given to appeal.