



MZALENDO

Data Protection Act 2019

Popular Version





About Mzalendo

Mzalendo ('Patriot' in Swahili) is a non-partisan project started in 2005 whose mission is to 'keep an eye on the Kenyan parliament.' Mzalendo site seeks to promote greater public voice and enhance public participation in politics by providing relevant information about the National Assembly and Senate's activities.

In 2010 The Omidyar Network awarded funding to mySociety to provide technical and administrative support to Mzalendo to help relaunch the site, drawing upon their experience in building sites such as TheyWorkForYou.

There are a number of further pages with more detailed information:

- [Site FAQs](#) straightforward answers to frequently asked questions about Mzalendo.com
- [Policies](#) provides details of the policies adhered to by Mzalendo.com and those it expects its users to adhere to
- [Partners](#) provides details of the partners involved in Mzalendo.com
- [Scorecard FAQs](#) straightforward answers to frequently asked questions about the scorecards on Mzalendo.com
- [Contact](#) provides details on how to contact Mzalendo.com



Contents

1. Introduction to Privacy and Data Protection in Kenya	1
2. Definitions	2
3. The Office of the Data Commissioner	4
4. Data Controllers and Data Processors	
5. Data Subjects	
6. Sensitive Personal Data.	
7. Transfer of personal data outside Kenya	
8. Exemptions	
9. Enforcement of Data Protection rights	



1. Introduction to Privacy and Data Protection in Kenya

Privacy

According to the Cambridge Dictionary, privacy is someone's right to keep their personal matters and relationships secret. The dictionary also describes it as the state of being alone.¹

In 1890, Samuel D. Warren and Louis Brandeis wrote an article titled "The Right to Privacy" for the Harvard Law Review where they argued that there is a "right to be left alone." This was in protest against the intrusive activities of the journalists of those days who used cameras to report in the printing press the lives of the high and mighty.

But when we refer to privacy, it is important that we distinguish between the different types of privacy. There is constitutional (also known as decisional or personal autonomy) privacy which is the freedom to make one's own decisions without interference by others in regard to matters seen as intimate and personal, such as the decision to use contraceptives or to have an abortion.

The second one is informational privacy which is concerned with an individual's ability to exercise control over access to their personal information. This may be the information one may post on social media or information in official documents. Informational privacy may be said to be a non-absolute moral right of persons to have direct or indirect control

over access to information about themselves, situations in which others could acquire information about oneself, and technology that can be used to generate, process or disseminate information about oneself.²

The Constitution of Kenya has the right to privacy. The Article contains both constitutional and informational privacy provisions which includes the right not to:

- (a) be searched. This includes one's home and property;
- (b) have one's possessions seized;
- (c) information relating to one's family or private affairs unnecessarily required or revealed; or
- (d) the privacy of one's communications infringed.³

Data Protection

Data Protection according to the Cambridge Dictionary are laws and regulations that make it illegal to store or share some types of information about people without their knowledge or permission.⁴ The Data Protection Act is a law that gives effect to Article 31(c) and (d) of the Constitution which are clauses on informational privacy. Therefore, we can say that the Act seeks to enable one to exercise control over the use of their personal information.

1. <https://dictionary.cambridge.org/dictionary/english/privacy>

2. <https://plato.stanford.edu/entries/it-privacy/>

3. Article 31 of the Constitution of Kenya

4. <https://dictionary.cambridge.org/dictionary/english/data-protection>

2. Definitions

The actors

The Data Commissioner: This is the person appointed to head the Office of the Data Commissioner. This term may be used to refer to the Office (just like the Attorney General or the Auditor General). The Office should be accessible to Kenyans in all parts of the country and it may establish directorates.

Data subject: This is an identifiable natural person who is the subject of personal data. Identifiable natural person in this case means a person who can be identified by reference to an identifier

such as a name, an identification number, location data, an online identifier or to factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity.

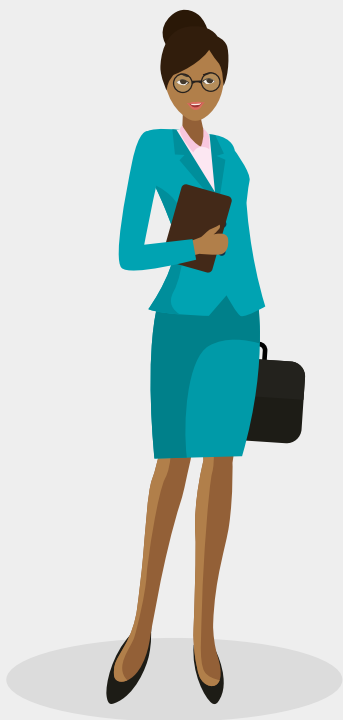
Data controller: This is a natural person, registered entity, public authority which determines the purpose and means of processing of personal data.






Data processor: This is a natural person, registered entity, public authority who processes personal data on behalf of the data controller.

Processing of personal data is any operation which is performed on personal data such as:




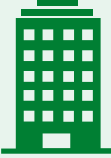
- collection, recording, organisation, structuring;
- storage, adaptation or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination, or otherwise making available; or
- alignment or combination, restriction, erasure or destruction.

Data Subject and personal data - the definition



-  a name
-  health data
-  location data
-  an online identifier
-  ID number

The Actors

-  Data Subject
-  Data Processor
-  Data Controller
-  Data Commissioner

6 Data Protection Act 2019

Popular Version

Objectives

The objective of the Data Protection Act is:

- to regulate the processing of personal data;
- to ensure that the processing of personal data is guided by data protection principles;
- to protect the privacy of individuals;
- to establish the legal and institutional mechanism to protect personal data; and
- to provide individuals with rights and remedies to protect their personal data from processing that is not in accordance with this Act.

The Concepts

Anonymisation: This is the removal, substitution or distortion of personal identifiers from personal data so that the data subject is no longer identifiable.

Biometric data: These are the physical, physiological or behavioral human characteristics including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition; that can be used to digitally identify a person to grant access to systems, devices or data.

Consent: This is permission for something to happen or agreement to do something. It means an express, unequivocal, free, specific and informed indication of an individual'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: Data is information which:

(a) is processed by programmed machines

(b) is recorded with the intention that it will be processed by programmed machines

(c) is recorded as part of a filing system

Encryption: This is the process of converting the content of any readable data using technical means into coded form so that its contents cannot be understood if intercepted. An example is when a confidential email is sent and the sender uses a program that obscures its content.

Filing system: This is any structured set of personal data which is readily accessible by reference to a data subject or according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Health data: This is data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates an individual subject to the provision of specific health services.

Personal data breach: This is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Profiling: This is the automated processing of personal data that involves recording and analysis of a person's psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people.

Pseudonymisation: This is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information. Such additional information must be kept carefully separate from personal data. Anonymization and pseudonymization are not the same methods. The main difference is that pseudonymization is a reversible process, unlike anonymization.

Register: This is the register kept and maintained by the Data Commissioner.

Restriction of processing: This is the marking of stored personal data with the aim of limiting their processing in the future.

Sensitive personal data: This is data that reveals an individual'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.

Third Party: This is a person or entity who under the direct authority of the data controller or data processor, is authorised to process personal data.

3. The Office of the Data Commissioner

Functions of the Office of the Data Commissioner are to:

- implement and enforce the Data Protection Act;
- establish and maintain a register of data controllers and data processors;
- oversee on data processing and ensure it is in accordance with the Data Protection Act;
- promote self-regulation among data controllers and data processors;
- conduct Data Protection Impact Assessments to ascertain that personal information is processed according to the law;
- receive and investigate any complaint on infringements of the rights under the Data Protection Act;
- to educate the general public on the provisions of the Data Protection Act;
- carry out inspections of public and private entities so as to evaluate the processing of personal data;
- promote international cooperation in data protection matters relating and ensure that Kenya complies with data protection obligations under international law;
- research on developments in data processing and ensure that they have no adverse effect on the privacy of individuals

Powers of the Office of the Data Commissioner

- To conduct investigations on their own initiative, or on the basis of a complaint
- To obtain necessary professional assistance, consultancy or advice when necessary

- To facilitate dispute resolution on disputes arising from the Data Protection Act
- To issue summons to a witness for the purposes of an investigation
- To require any person to provide it with explanations, information and assistance
- To impose administrative fines for failures to comply with the Data Protection Act
- The Data Commissioner may join associations and organisations in furtherance of the Act.

Codes, guidelines and certification.

The Data Commissioner may:

- issue guidelines or codes of practice for the data controllers, data processors and data protection officers
- offer data protection certification standards and data protection seals and marks in order to encourage compliance of processing operations with the Data Protection Act
- require certification or adherence to code of practice by a third party

develop sector specific guidelines for areas such as health, financial services, education, social protection and any other areas



4. Data Controllers and Data Processors

Registration of Data Controllers and Data Processors

No person or entity is allowed to be a data controller or data processor unless they have registered with the Data Commissioner. The Data Commissioner shall provide thresholds required for mandatory registration of data controllers and data processors.

Data controllers or data processors are required to apply for registration to the Data Commissioner. Where an applicant has met the requirements for registration, the Data Commissioner shall issue them a certificate of registration. The duration of validity of the registration certificate shall be determined at the time of the application and the holder may apply for a renewal of the certificate upon expiry.

The Data Commissioner in maintaining the Register will be making any changes on the particulars of registration as submitted by the data controller or data processor. The Data Commissioner may also remove any entry in the register which has ceased to be applicable at the request of a data controller or data processor.

The Register shall be a public document; hence it will be available for inspection by anyone. A person may request the Data Commissioner for a certified copy of an entry in the register.

The Data Commissioner may vary the terms and conditions of the certificate of registration or cancel a registration certificate upon issuance of a notice to show cause. This may be done where in-

formation given by the applicant is false or the holder of the registration certificate fails to comply with the Act.

The Data Protection Officer

A data controller or data processor may appoint a data protection officer where:

- processing is carried out by a public or private body,
- the core activities of the data controller or data processor consist of regular and systematic monitoring of data subjects, and;
- where the processing of sensitive categories of personal data is taking place.

Duties of the Data Protection Officer:

- advise the data controller or data processor and their employees on data processing requirements provided by the law
- ensure that the data controller or data processor complies with the Data Protection Act
- facilitate capacity building of staff involved in data processing operations
- provide advice on data protection impact assessment; and
- co-operate with the Data Commissioner on matters relating to data protection.

Obligations of Data Controllers and Data Processors

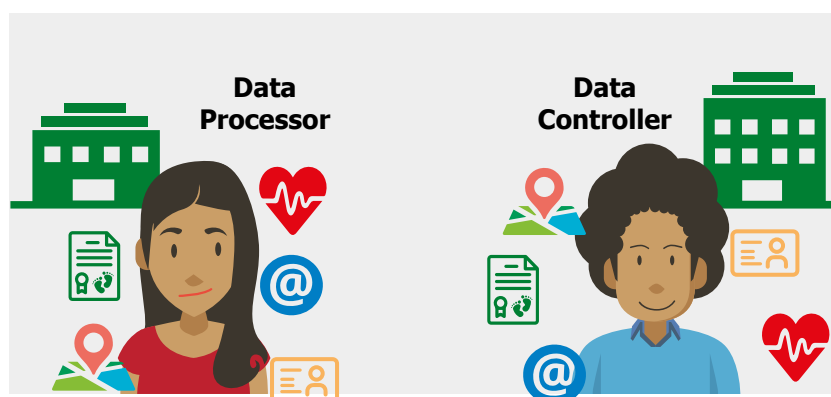
Data Protection Impact Assessment.

A Data Protection Impact Assessment (DPIA) is a process which helps a data controller or data processor to identify and minimise the data protection risks of a data processing project. A DPIA must be done where data processing is likely to risk the rights and freedoms of individuals.

A data protection impact assessment (DPIA) must:

- describe the nature, scope, context and purposes of the data processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to the rights and freedoms of individuals; and
- identify any additional measures to mitigate those risks.

Data controllers or data processors should consult the Data Commissioner sixty days before they start data processing if a data protection impact assessment shows that the processing would result in a high risk to the rights and freedoms of an individual.



Duty to notify.

Entities should, before collecting personal data:

- inform individuals of their rights under the Data Protection Act,
- that their personal data is being collected,
- why it is being collected,
- the third parties who will process the data and the safeguards in place,
- the technical and organizational security measures taken,
- whether data collection is in compliance to any law, if it is voluntary or mandatory, and;
- the consequences of an individual failing to provide the requested data.

Data protection by design or default.

Data protection by design is an approach that ensures a data controller or data processor considers privacy and data protection issues at the design phase of any system, service, product or process and then throughout the data lifecycle.

Data protection by default requires a data controller or data processor to ensure that they only process the data that is necessary to achieve their specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation.

Data protection by design or default involves putting in place appropriate technical and organisational measures designed to implement the data protection principles effectively and safeguard individual rights. There is no 'one size fits all' method to do this as it all depends

on a data controller or data processor's circumstances.

Notification and communication of breach.

A data controller should notify the Data Commissioner within seventy-two hours (72 hours) of becoming aware of such breach that there has been a personal data breach. The data controller is also obligated to notify the affected individual in writing within a reasonably practical period that there has been a personal data breach.

5. Data Subjects

Principles of personal data protection

The Data Protection Act has eight key principles. These principles require every data controller or data processor to ensure that:



Right to privacy

The processing of personal data is in accordance with the right to privacy of the individual.



Lawfulness, fairness and transparency

The processing is lawful, fairly and transparent.



Data minimisation

The collection of personal data is adequate, relevant, limited to what is necessary in relation to the purposes for which it is being processed. Personal data on family or private affairs is collected only after a valid explanation is provided whenever such information is required



Purpose limitation

The collection of personal data is for explicit, specified and legitimate reasons and no further processing in a manner incompatible with those purposes



Accuracy

Personal data is accurate, up to date with measures to ensure inaccurate personal data is erased or rectified



Storage limitation

Personal data is not kept for longer than is necessary in a form which identifies an individual.



Data Localisation

Personal data is not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the individual

Rights of a data subject

An individual has the following rights as a data subject:

i. The right to be informed on the use of their personal data



ii. The right to access their personal data in custody of data controller or data processor



iii. The right to object to the processing of all or part of their personal data



iv. The right to correction of false or misleading data about them



v. The right to deletion of false or misleading data about them.



Other rights are:

The right to restrict processing

The right to data portability

Rights in relation to automated decision making and profiling.

Special exercise of data subject rights

Due to lack of capacity, a child's data subject rights may be exercised by a parental authority or by a guardian. This is also the same for persons living with a mental disability or other disability. They can exercise their data subject rights through a guardian or administrator.

An individual is allowed to authorize another person to exercise their data subject rights.

Collection of personal data

Personal data should be collected directly from an individual by a data controller or data processor.

Instances where personal data may be collected indirectly are where:

- (a) the data is in a public record
- (b) the individual has made the data public
- (c) the individual has consented to the collection of personal data from another source
- (d) the individual is incapacitated and the guardian has consented to the collection
- (e) the collection from another source would not affect the interests of the individual
- (f) the collection of personal data from another source is necessary for criminal procedure, enforcement of a law that imposes a fine or for the protection of human rights.

Duty to notify

Before collecting personal data, a data controller or data processor should inform an individual of:

- a) their rights as a data subjects
- b) that their personal data is being collected

- c) the purpose for the collection of personal data
- d) the third parties who the personal data will be transferred to and the safeguards in place
- e) the contacts of the data controller or data processor
- f) a description of the technical and organizational security measures in place for the data
- g) the data being collected in compliance to a law, the voluntary and mandatory
- h) the consequences of failing to provide all or any part of the requested data.

Lawful processing of personal data

A data controller or data processor should not process personal data, unless an individual has consented to the processing. The exception to this rule is when the processing is necessary for:

- the performance of a contract to which the individual a party or for pre-contractual purposes
- compliance with any legal obligation
- to protect the interests of the individual or another natural person;
- the performance of a task carried out in the public interest
- legitimate interests pursued by the data controller or data processor by a third party to whom personal data is disclosed,
- the purpose of historical, statistical, journalistic, literature and art or scientific research.

A breach of this is a criminal offence.

Consent

Since all data processing has to be consented, data controllers and data processors bear the burden of proof for establishing that an individual consented to the processing of their personal data.

An individual has the right to withdraw consent at any time. However, withdrawal of consent does not affect the lawfulness of previously consented data processing.

A child's personal data

Data controllers and data processors should only process a child's personal data after getting consent from the child's parent/ guardian and, if the processing is in the best interest of the child.

Data controllers and data processors should ensure that they have appropriate age verification and consent mechanisms to enable them process the personal data of a child.

Data controllers and data processors who provides counselling or child protection services to a child may not be required to obtain parental consent.

Restriction on personal data processing

An individual may request a data controller or data processor to restrict the processing of personal data where:

- they are contesting the accuracy of the personal data
- the personal data is no longer required for processing, except for the exercise or defence of a legal claim
- processing is unlawful and the individual opposes the erasure and requests restriction of its use instead
- an individual has objected to the processing, pending verification as to whether the legitimate interests of the data controller or data processor overrides those of the data subject.

Where processing of personal data has been restricted, the personal data

12 Data Protection Act 2019

Popular Version

should be processed with the individual's consent, for the exercise or defence of a legal claim, the protection of a right and for reasons of public interest. A data controller should inform an individual before withdrawing the restriction on processing of the personal data.

To enable the exercise of this right, a data controller or data processor should implement mechanisms to ensure that time limits established for the rectification, erasure or restriction of processing of personal data are adhered to.

Automated individual decision making

Automated individual decision-making is where a decision made by automated means without any human involvement. Instances of automated decision making in Kenya are include:

- an decision to award a loan on a mobile lending application
- the automated school selection system in NEMIS; and
- online recruitment aptitude tests.

Every individual has a right to not be subjected to a decision based solely on automated processing, including profiling, which produces legal effects without human intervention.

This right will not apply where the decision is:

- necessary for a contract between the individual and a data controller;
- authorised by a law which lays down measures to safeguard the individual's rights,
- based on the individual's consent.

In the event a data controller or data processor takes an automated processed decision, which produces legal

effects on an individual, they should notify the individual and allow them time to appeal/review. The individual can at this point ask the data controller or data processor to reconsider the decision or to make a new decision that is not based solely on automated processing.

Objecting to processing

An individual has a right to object to the processing of their personal data. This right is limited where the data controller or data processor demonstrates that there is a legitimate interest for the processing which overrides the individual's interests, or for the exercise of a legal claim.

Personal Data processing for Direct Marketing

A data controller or data processor should not use personal data for commercial purposes unless they have sought and gotten express consent from an individual or are authorized by the law and have informed the individual of such use.

When using personal data for commercial purposes, they should anonymise the data where possible.

Right to data portability

An individual has the right to receive their personal data in a structured, commonly used and machine-readable format from a data controller or data processor and to transmit the data to another data controller or data processor without any hindrance. Where technically possible, the personal data should be transmitted directly from one data controller or processor to another.

This right is limited where processing is necessary for public interest or it may

adversely affect the rights and freedoms of others.

Limitation to retention of personal data

Data controllers or data processors should only retain personal data for the period which it is necessary to satisfy the purpose for which it is processed.

The limitation to this rights is where the retention is:

- (a) required or authorised by law;
- (b) necessary for a lawful purpose;
- (c) consented by the individual/data subject; or
- (d) for historical, statistical, journalistic literature and art or research purposes.

Right of rectification and erasure

An individual may request a data controller or data processor to rectify personal data in its possession that is inaccurate or outdated.

An individual may also request a data controller or data processor to erase personal data that they obtained unlawfully, is irrelevant to them and they are no longer authorised to retain'

If the data had been transmitted to a third-party, the data controller or data processor should take reasonable steps to inform the third parties the individual has requested a rectification or an erasure.

6. Sensitive Personal Data

Grounds for processing sensitive personal data

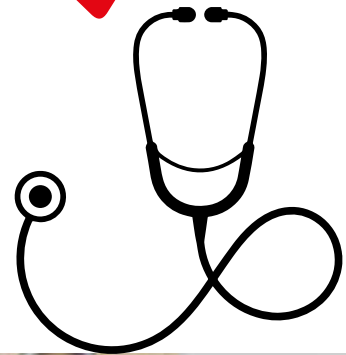
The sensitive personal data of an individual may be processed where:

- legitimate activities with appropriate safeguards.
- the processing relates to personal data which is manifestly made public by the individual.
- processing is necessary for defence of a legal claim, carrying out the obligations of the controller or for protecting the vital interests of the individual who incapable of giving consent.

Personal data relating to health

Personal data relating to the health of a data subject may only be processed by a health care provider or by a person subject to professional confidentiality obligations under any law. This can only be done where it is necessary for public health or by a person who owes a duty of confidentiality under any law.

The Data Commissioner is empowered to prescribe further categories of personal data which may be classified as sensitive personal data.



7. Transfer of personal data outside Kenya

Conditions for personal data transfer out of Kenya

Data controllers and data processors can only transfer personal data to another country where they have proved to the Data Commissioner that, there are appropriate safeguards for the security and protection of the personal data such as data protection laws. The other condition is when the transfer is necessary for the performance of a contract, for a matter of public interest, for the defence of a legal claim and to protect the interests of an individual or other persons.

Safeguards prior to transfer of personal data out of Kenya

The processing of sensitive personal data out of Kenya should only be done after obtaining consent of an individual and the confirmation of appropriate safeguards.

The Data Commissioner can request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests.

Data transfer conditions



Consent



Presence of safe guards in destination country



8. Exemptions



General exemptions

The processing of personal data is exempt from the provisions of the Data Protection Act if:

- (a) it is by an individual as a personal or household activity
- (b) it is necessary for national security or public interest
- (c) disclosure is required by or under any written law or by an order of the court.

The Data Commissioner may prescribe other exemptions to the Data Protection Act.



Research, history and statistics

Further processing of personal data will be deemed to be compatible with the purpose of collection if the data is used for historical, statistical or research purposes. Data controllers and data processors should ensure that the records are not being used for any other purposes and that the data is anonymised.

The Data Commissioner is expected to prepare a code of practice containing practical guidance on the processing of personal data for purposes of Research, History and Statistics.



Journalism, literature and art

Processing of personal data for the publication of a literary or artistic material which would be in public interest is exempted from the provisions of the Data Protection Act.

The Data Commissioner is expected to prepare a code of practice containing practical guidance on the processing of personal data for purposes of Journalism, Literature and Art.



Data-sharing code for government agencies

The Data Commissioner may issue a data sharing code which will contain a practical guidance on the sharing of personal data according to provisions of the Data Protection Act. The data sharing code will specify on the lawful exchange of personal data between government departments or public sector agencies. The Commissioner may also issue guidance that promotes good practice in the sharing of personal data.

9. Enforcement of Data Protection rights



Complaints to the Data Commissioner

A person who is aggrieved by issue that relates to the Data Protection Act can lodge a complaint with the Data Commissioner orally or in writing. Complaints made to the Data Commissioner should be investigated and concluded within ninety days.



Investigation of complaints

The Data Commissioner for the purpose of investigating a complaint, may order any person:

- to appear for the purpose of being examined orally
- produce such book, document, record or article as may be required for the investigation
- furnish a statement in writing made under oath setting out all information required

Where material relevant to an investigation consists of information stored in any mechanical or electronic device, the Data Commissioner may require the person named to produce or give access to it in a form in which it can be taken away and in which it is visible

A person who refuses to comply with a notice, or who furnishes to the Data Commissioner any information which is false or misleading, commits an offence.



Enforcement notices

The Data Commissioner is empowered to issue an enforcement notice to any person that is not complying with the provisions of the Data Protection Act. An enforcement notice served on a person should contain the specify the provision in the Act which has been contravened, the measures to be taken to remedy the situation, the period within which those measures should be implemented and the right of appeal.

Any person who fails to comply with an enforcement notice commits an offence and is liable on conviction to a fine not exceeding (Ksh. 5,000,000) five million shillings or to imprisonment for a term not exceeding (2) two years, or to both.



Power to seek assistance

The Data Commissioner may seek the assistance of any person or authority as is reasonably necessary to assist the Data Commissioner in the discharge of their functions.



Power of entry and search

The Data Commissioner, upon obtaining a warrant from a Court, may enter and search any premises for the purpose of discharging any function under the Data Protection Act.



Obstruction of Data Commissioner

A person who obstructs or impedes the Data Commissioner, fails to provide assistance or information requested by the Data Commissioner, refuses to allow the Data Commissioner to enter any premises or gives to the Data Commissioner information which is false commits an offence and is liable on conviction to a fine not exceeding (Ksh. 5,000,000) five million shillings or to imprisonment for a term not exceeding (2) two years, or to both.



Penalty notices

The Data Commissioner has the power to issue a penalty notice requiring a person who is breaching the Act to pay to the Office of the Data Commissioner an amount specified in the notice.



Administrative fines

In relation to an infringement of a provision of this Act, the maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is up to five million shillings, or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower.



Right of appeal

A person against whom administrative action has been taken by the Data Commissioner (including in enforcement and penalty notices) may appeal to the High Court.



Compensation to a data subject

An individual who suffers damage by reason of a contravention of the Data Protection a requirement of this Act is entitled to compensation for that damage from the data controller or the data processor. Damage in this context is financial loss and damage not involving financial loss, including distress.



Preservation Order

The Data Commissioner may apply to a court for a preservation order for the expeditious preservation of personal data including traffic data, where there is reasonable ground to believe that the data is vulnerable to loss or modification.



Offences of unlawful disclosure of personal data

Data controllers or data processors who, without lawful excuse, disclose personal data in any manner that is incompatible with the purpose for which such data has been collected commit an offence.

- A person who obtains access to personal data without authority of the

data controller or data processor by whom the data is kept commit an offence.

- A person who discloses personal data to third party, commit an offence.
- A person who offers to sell personal data where such personal data has been obtained in breach of a data base commits an offence.



General penalty.

A person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, be liable to a fine not exceeding three million shillings or to an imprisonment term not exceeding ten years, or to both. The court may also order the forfeiture of any equipment connected with the commission of the offence and prohibit the doing of any act to stop a continuing contravention.



MZALENDO

Data Protection Act 2019

Popular Version

