MACRA

Malawi Government

PERSONAL DATA PROTECTION HANDBOOK

About this Handbook

MACRA

This handbook highlights legal and institutional mechanisms for the protection of personal data in Malawi. It states the key principles of personal data protection; the definitions of commonly used technical terms in data protection frameworks; and explains the definition of personal data and types of personal data; and gives practical advice on how to comply with the Data Protection Act, 2024.

Foreword

By MACRA Director General
(The designated Data Protection Authority in Malawi)

As the Director General of MACRA, the designated Data Protection Authority in Malawi, I am pleased to introduce this handbook on the Data Protection Act in our country.

On 1st February 2024, His Excellency the President of the Republic of Malawi Dr Lazarus McCarthy Chakwera assented to the Data Protection Bill, marking a significant milestone in our efforts to safeguard the fundamental rights and freedoms of individuals with respect to the processing of their personal data.

In today's digital age, the collection, storage, and use of personal information have become pervasive across various sectors.

It is crucial that we establish robust data protection frameworks to ensure that individuals' personal data is handled in a fair, lawful, and transparent manner. The Data Protection Act provides the necessary legal and regulatory mechanisms to achieve this goal.

This handbook serves as a valuable resource for organizations, policymakers, and individuals alike. It provides an overview of the Act, outlining the key principles, the rights of data subjects, the obligations of data controllers and processors, as well as the enforcement and compliance mechanisms.

The practical guidance included in this handbook will greatly assist in the effective implementation of the Act and contribute to a culture of data protection in Malawi.

I commend the efforts of the team responsible for compiling this comprehensive and user-friendly handbook.

It is my hope that this resource will empower all stakeholders to fully understand and uphold the provisions of the Data Protection Act, thereby strengthening the protection of personal data and maintaining the trust of Malawian citizens in the digital landscape.

Together, let us work towards a future where the fundamental right to privacy is respected, and the personal data of all Malawians is safeguarded with the highest standards of care and diligence.

Daud Suleman
Director General
Malawi Communications
Regulatory Authority (MACRA)

Introduction to Personal Data Protection

Personal Data protection in Malawi is governed by the Data Protection Act of 2024. The Act protects personal data by establishing checks and balances aimed at protecting individuals whenever their personal data is being processed. The Act requires that organizations processing personal data must do so lawfully, fairly, and in a transparent manner. The Act further recognizes the need for an independent supervisory body to oversee and ensure the protection of personal data.

The Malawi Communications Regulatory Authority (MACRA), as the Data Protection Authority, is responsible for ensuring compliance with the provisions of the Act. As the designated Data Protection Authority, MACRA plays a vital role in safeguarding the rights of data subjects.

The Act empowers data subjects to have greater autonomy and control over their personal information. A data subject is a natural person to whom personal data relates.

Apart from providing safeguards in the manner in which personal data is processed, the Act goes on to give the data subject certain rights that are exercisable against organizations that collect and process their data. Such rights include the right to access the data, to have it rectified where there are errors, and the right to have the data erased where further processing of the data is no longer necessary. The Act also provides for redress where there has been a data breach and non-adherence to the data protection principles and mechanisms put in the Act. Individuals now have the tools to assert their digital rights.

The Act mandates data controllers and processors to adhere to stringent obligations, including recording all data processing activities, implementing data security measures, and notifying both the Authority and data subjects in the event of data breaches.

Importantly, the Data Protection Act extends its horizon beyond domestic borders by regulating cross-border transfers of personal data. As a principle, the Act allows the exporting of personal data outside of Malawi only where such data will be afforded adequate protection in the destination country.

Furthermore, the Act recognizes that certain organizations collect and process significant amounts of personal data. Greater processing of personal data comes with greater and significant risk to such personal data. The Act has categorized these as data processors of significant importance and has placed stricter and additional obligation on them to ensure that they uphold the highest standards of data protection.

By holding these entities accountable and imposing penalties for non-compliance, the legislation seeks to instill a culture of responsibility and integrity in data management practices.

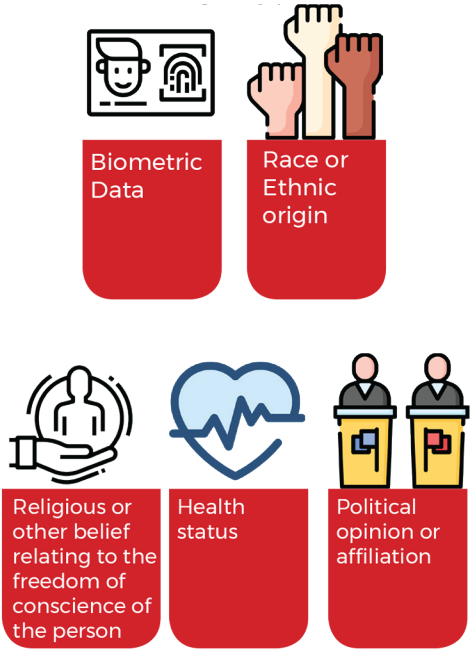
The Data Protection Act empowers MACRA, as the Data Protection Authority, to enforce and issue compliance orders to entities that contravene the provisions of the Act. To protect personal information of individuals and to avoid potential penalties for non-compliance, it is important for organizations in Malawi to be aware of their obligations and comply with the provisions of the Act. It is also important for individuals to be mindful of their own personal data privacy and protection.

What is personal data?

Personal data is defined as any data relating to an identifiable natural person directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that person.

What is sensitive personal data?

Sensitive personal data is information that is very private and needs to be stringently protected under the law.
Sensitive personal data relates to a person's—



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

Why Personal data protection is critical?

Failing to protect personal information can have serious consequences:

01 It can lead to identity theft.

02 It can lead to financial fraud.

03 It can lead to unauthorized surveillance.

04 It can damage an individual's reputation.

05 It can lead to unauthorized disclosure of private and confidential information.

06 It can result in a loss of trust and confidence in an organization.

Organizations have legal and ethical obligations to protect personal data.

Who is a Data Subject

This is a natural person to whom particular personal data relates. It is you and me. Personal Data protection is about protecting the personal data of that data subject and giving him rights to have a greater say on how his personal data is collected and used.

Who is a Data Controller?

A Data Controller is a natural or legal person who, alone or jointly with another natural or legal person, determines the purpose (the why) and means (the how) of processing personal data.

Data Controller Examples

- A bank collecting personal information from customers to open new accounts
- A retail company collecting personal information from customers
- A hospital collecting personal information from patients
- A government agency collecting personal information from citizens
- A credit bureau collecting personal information from financial institutions

Who is a Data Controller of significant importance.

This is a data controller who—

(a) is domiciled, ordinarily resident, or ordinarily operates in Malawi and processes or intends to process personal data of more than ten thousand data subjects who are resident in Malawi; or

(b) processes or intends to process personal data of significance to the economy, society, or security of Malawi.

Who is a Data Processor?

This is a natural or legal person who processes personal data on behalf of a data controller.

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 service processing medical claims for a hospital.
- A tax preparation software provider processing tax returns for a government agency.

Data Controller vs Data Processor

A clear distinction is made between a data controller and a data processor. The responsibilities for each in respect to personal data protection therefore differs.

A data controller determines the reason for processing personal data and how the processing should be done. The data controller decides what information is captured and why. The data controller is ultimately responsible for the compliance with data protection principles and the compliance of data processors it engages to process personal data on its behalf. Its other responsibilities include responding to the rights of data subjects, implementing data security measures, and managing data breaches.

A data processor on the other hand has less control over the personal data it processes on behalf of the data controller. It still has obligations and responsibilities which include processing personal data according to the instructions of the data controller, enforcing security measures and notifying the data controller of any personal data breach.

Principles of Personal Data Protection

1.
The overarching principle is that personal data must be processed lawfully, fairly and in a transparent manner.

2.
Lawfulness: an organisation must have one of the following as a legal basis for processing personal data:

(a) **Consent:** of the individual to the processing of their personal data.
(b) **Contractual necessity:** processing is needed in order to enter into or perform a contract.
(c) **Legal obligation:** for which the organisation is obliged to process personal data for pursuant to a statutory obligation or an order made by a court of law.
(d) **Vital interest:** of individuals, where processing is necessary to protect their lives.
(e) **Public interest:** specific to organisations exercising official authority or carrying out tasks in the public interest.
(f) **Legitimate interest:** of the organisation or the third parties engaged.

Tips:
-An organisation must first determine the lawful basis before it begins to process personal data and must document it.

-Should the purpose for processing changes, the organisation must reassess the new purpose and determine a valid lawful basis.

3.
Purpose Limitation: Personal data should be collected for a specific and legitimate purpose.

4.
Data Minimization: Only collect and process personal data that is adequate, relevant, and limited to the specific purpose for which it was collected.

5.
Data accuracy: Ensure that personal data to be processed is accurate and, where necessary, is up-to-date.

6.
Storage Limitation: Do not store personal data for a period that is longer than necessary to achieve the purpose for which the data was collected or processed.

7.
Data integrity and data confidentiality: Ensure that the appropriate technical or organizational security measures are implemented to guarantee the security of personal data.

8.
Determining the validity of consent: Obtain the consent of a data subject; or where a child or a person who is not capable of providing consent, obtain the consent of the legal guardian.

9.
Provision of information to a data subject: A data subject should be provided with information such as identity and contact details of the data controller or representative; legal basis for processing the personal data; the purpose; and storage period.

10.
Processing personal data of children and other legally incapacitated persons: Where a data subject is a child or any other natural person lacking the legal capacity, a parent or legal guardian, shall exercise the rights of the data subject on behalf of the data subject.

11.
Processing of personal data relating to criminal offences, convictions: Not to process personal data relating to a criminal offence, conviction, or security measure imposed on the data subject unless:

- the processing is authorised under a written law and the law provides for necessary safeguards of the rights and freedoms of the data subject; or
- where the processing is done under the authority of a Government organ or other official authority.

Processing sensitive personal data

Data Controllers and Processors can only process sensitive personal data if there's a good reason, such as:

- The data subject has provided consent
- To protect the interest of the data subject
- For exercising or performing a right or obligation of the data controller, data processor or data subject under a written law or a court order
- Is in the interest of public health
- Is for public interest
- For legal purposes
- For the purpose of archiving the data for public interest or for research or statistical purposes
- The data subject has intentionally made the data public
- The data controller or data processor is a foundation, association, or any other not-for-profit body with a charitable, educational, literary, artistic, philosophical, religious or trade union

Where sensitive personal data is processed, the data controller or data processor shall put in place appropriate measures to safeguard the fundamental rights and interests of the data subject

Data subject rights

- To obtain confirmation of whether his/her personal data is being processed.
- To be informed of the use of their personal data.
- To access their personal data in custody of Data Controller or Data Processor.
- To object to the processing of all or part of their personal data.
- To have any error in personal data rectified by the Data Processor.
- To erasure of personal data.
- Not to be subject to a decision based solely on automated processing of personal data.

Restrictions to data subject rights

The rights of a data subject are restricted where the processing of the personal data of the data subject is for the purpose of—

- National security.
- The prevention, investigation, detection or prosecution of a criminal offence or the execution of a criminal penalty.
- Pursuing a national economic or financial interest, including a monetary, budgetary and taxation matter.
- Public health.
- Social security.
- Judicial proceedings.
- The prevention, investigation, detection, and prosecution of a breach of ethics for a regulated profession.
- Monitoring, inspection, or exercise of a regulatory function by a public authority.
- Protecting the data subject or the rights and freedoms of another person
- The enforcement of a civil law claim.

Personal Data Protection Compliance

Data Controllers or Processors can take the following steps to ensure compliance:

- Data Controllers and Data Processors of significant importance must register with the Authority before undertaking any processing activities.
- Renew the certificate upon expiry.
- Appointing a personal data protection officer.
- Implement data protection principles and ensure compliance.
- Ensure that the processing of personal data is carried out lawfully.
- Carry out data protection impact/risk assessments.
- Implement appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, or destruction.
- Report data breaches to the Data Protection Authority data commissioner within 72 hours.
- Ensure appropriate safeguards are in place for the transfer of personal data outside Malawi.

Why data controllers and data processors of significant importance should Register with the Data Protection Authority?

- Data Controllers and data processors in this category cannot process any personal data unless they are registered.
- Closer collaboration with the Authority and this enhances the protection of personal data.
- Helps build trust and confidence in an organization.
- Helps prevent negative publicity and protect an organization's brand image.
- Helps improve data management practices and ensures that personal data is accurate and up-to-date.

Registration process

1. Submit an application in the prescribed form accompanied by prescribed fee.
2. The Authority, within fourteen days, registers the data controller or data processor or refuse.
3. The Authority prescribes terms and conditions on the registration.
4. The Authority shall keep and maintain a register of Data Controllers and Processors.
5. A registered Data Controller or Processor has obligation to notify the authority of change of registration details within ninety days of the change.
6. The Authority issues a registration certificate.

Suspension of Registered Data Controllers/Processors

The Authority may suspend or cancel the registration of a Data Controller or Data Processor when—

- There is no compliance with any provision of the Data Protection Act.
- There was a misleading or false representation at the time of registration.
- Where there is noncompliance with the terms and conditions set by the Authority for the registration certificate.

Complaints

A complaint is a statement expressing dissatisfaction with the way personal data has been handled.

- Lodge a complaint, in writing, with the Authority.
- Parent or legal guardian may lodge a complaint, in writing, with the authority on behalf of a child or any other person lacking legal capacity.
- The complaint should be lodged within ninety days of the action or inaction.
- Provide personal information including: full name, ID/passport number, postal address, age & gender, and phone number.
- Provide information about the respondent, including: names and contact details, date of occurrence of the alleged infringement, nature of the complaint, any potential or actual harm or urgency, and any supporting documents.
- The Authority investigates the complaint.
- The Authority may, on its own initiative, investigate any matter where the Authority believes that the Act has been contravened, or is likely to be contravened.
- The Authority, within thirty days of completing investigation, communicates the results the parties concerned.
- The Authority issues an appropriate compliance order.

Who can complain?

- The Data Subject in person.
- A person acting on behalf of the Data Subject.
- Any other person authorized by law to act on behalf of a data subject.
- Anonymously.

Goals of investigations by the Authority:

To gather all relevant facts concerning the 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 wrong doing from happening again?

Investigative powers of the Data Protection Authority

For the purpose of the investigation of a complaint, the Authority may order any person to:

- Attend before the Authority at a specific time and place to be examined orally.
- Produce any document, record, or article, with respect to any matter relevant to the investigation.
- Furnish a statement, in writing, made under oath.
- Where material consists of information stored in any mechanical or electronic device, the Authority may require the person in custody of the information to produce, or give the Authority access to, the information.

Enforcement

On the completion of an investigation, any corrective action, if necessary, will be by an Enforcement Order, which may include:

- Compensation to a data subject.
- Account for profits made out of the contravention.
- An administrative penalty not exceeding **K20,000,000**.

MACRA

1st Floor, Green Heritage House
2 Khonje Close
City Centre
P.O Box 30214
Lilongwe, MALAWI
Postcode: 207213

Phone Numbers:
+265 111 77 55 34 | +265 111 77 55 35
+265 111 77 55 33

dg@macra.mw

www.macra.mw