

Malawi Communications Regulatory Authority

Guidelines and Checklist on Compliance with the Data Protection Act 2024

The Authority issues this document as a source of information and guide to data controllers and processors and interested parties of the general public. For this reason it should not be relied on as legal advice or regarded as substitute for legal advice in individual cases. The information contained in this document may be subjected to changes from time to time.

Table of Contents

Introduction.....	1
Application of the Act	1
Personal data and data processing	1
Geographic scope.....	2
Grace period	2
Two years for other data controllers and data processors	2
Immediate application	4
data controllers and processors of significant importance	4
other data controllers and data processors.....	4
Data controllers and processors	5
Distinction between data controllers and data processors	5
Relationship between data controllers and data processors.....	5
Responsibilities and Duties of data controllers and data processors	6
Compliance with data protection principles.....	8
Reviewing data processing activities.....	8
Establishing lawful basis of processing.....	9
Demonstrating consent.....	10
Specifying purpose of data processing, minimization and accuracy.....	10
Data storage	11
Data protection impact assessment (DPIA)	11
Data subjects.....	12
Disclosures to data subjects at the time of collecting the personal data.....	12
Honouring the rights of data subject.....	13
Data security	14
Measures for protecting data	14
Notification of personal data breaches	15
Transferring personal data abroad.....	16
Cross-border data transfers.....	16
Organisational readiness	17
Establishing internal governance	17
Training	17

Introduction

The protection of personal data is vital to the development of Malawi's digital economy and protection of its population. Malawi citizens need to have confidence in how information about them is used, that it is kept secure, and that it is not collected to invade their privacy and undermine their personal liberties.

The Malawi Communications Regulatory Authority (hereinafter referred to as "the Authority") as the designated Data Protection Authority is mandated by the Data Protection Act (No. 3 of 2024) (the "Act") to promote the protection of personal data, regulate the processing of personal data throughout Malawi and oversee the implementation of and be responsible for the Act.

The Act requires companies, business partnerships and other private sector organisations, Government Ministries, Departments and Agencies, as well as non-governmental organisations in the Malawi economy, to revise how they handle data about people. They will need to review the purposes for which they collect personal data, how they process it, how they protect it, how they reuse it, where they store and transfer it, to whom they transfer it for processing, and how they outsource data processing to third parties. They will need to assess the sensitivity of the personal data they process and prepare to apply tighter protections to such data.

The Act also provides rights to individuals (referred to as data subjects) to ensure that personal data relating them are properly managed.

These Guidelines provide an overview of the requirements likely to affect most organisations. They aim at helping organisations understand potential gaps they may have in compliance and the steps that they will have to take to meet those requirements.

Organisations that are domiciled, ordinarily resident, or ordinarily operating in Malawi and currently process or intend to process personal data of more than 10,000 data subjects who are within Malawi have special obligations to register with the Authority and pay certain fees.

The guideline and checklist below provide references to sections in the Act, summarises key requirements and provisions of the Act, and provides guidance and recommendations as to what should be done to comply with the Act. It also suggests which teams in a given organisation might appropriately be involved in such actions:

Legal & compliance



Technical & IT



Customer relations



Public relations



HR



DRAFT

Application of the Act

s.2, s.3

Personal data and data processing



The Data Protection Act applies to processing of personal data:

- Personal data is defined as any data relating to an identifiable natural person which, 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; and
- Processing is also defined as any operation, or set of operations, performed on personal data, whether or not by automated means, and includes collection, recording, organization, structuring, storage, alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data;
- The Act does not apply to:
 - the processing of personal data by a natural person in the course of performing a solely personal, recreational or household activity; and
 - the mere transmission of personal data through Malawi.

Organisations should consider:

- whether they deal with information relating to individuals who can be identified by name, identification number, location, or any other features;
- what activities they perform in relation to that data; and
- Consequently decide, whether they are processing personal data.

s.3

Geographic scope

The Data Protection Act applies where there is:

- the processing of personal data in Malawi by a data controller or data processor domiciled, ordinarily resident or operating in Malawi;
- the processing of personal data of a data subject who is within Malawi, by a data controller or data processor who is domiciled, ordinarily resident or operating outside Malawi, and the data processing relates to the:
 - offering of goods or services, irrespective of whether the data subject is required to pay for the goods or services; or
 - monitoring of the behavior of the data subject, as far as the behaviour takes place within Malawi;
- the processing of personal data in Malawi, whether wholly or partly by automated means or by other means other than automated means, which forms or is intended to form part of a filing system.

Organisations should:

- verify that they are domiciled, ordinarily resident or ordinarily operating in Malawi;
- verify that they are monitoring or targeting data subjects in Malawi;
- verify that data processors processing personal data on their behalf are domiciled, ordinarily resident, ordinarily operating, or monitoring or targeting data subjects in Malawi such that the data processing would fall within the scope of the Data Protection Act; and
- where the entity or activity falls within the geographic scope, ensure that the processing of personal data complies with the Act.

s.53

Grace period

Two years for other data controllers and data processors

(a data controller or a data processor who is domiciled, ordinarily resident, or ordinarily

Organisations should verify:

- where they are domiciled, ordinarily resident or ordinarily operating;
- whether they qualify as data controllers or processors of significant importance.

operates in Malawi and—

- is not a data controller of significant importance or data processor of significant importance shall be exempt from compliance with this act, for a period of twenty-four months from the date the act comes into operation; or
- is a data controller of significant importance or data processor of significant importance shall, within six months from the date the act comes into operation, comply with the requirements prescribed under this act.)

The Data Protection Act provides a two- year grace period for Malawi data controllers and processors that are not deemed to be of “major importance” (see below). Specifically, it exempts all data controllers and processors that are domiciled, ordinarily resident, or ordinarily operating in Malawi and that are not data controllers or processors of major importance. However, the Act will apply to all non-Malawi data controllers and processors as soon as it enters into force.

s.3,
s.41,
s.52,
s.53

Immediate application

data controllers and processors of significant importance

The Data Protection Act applies immediately to data controllers or data processors domiciled, ordinarily resident, or ordinarily operating in Malawi and processing or intending to process personal data of more than 10,000 data subjects who are within Malawi. It also applies to data controllers and data processors that process or intend to process personal data of significance to the economy, society or security of Malawi.

The data controllers or data processors must register with the Authority and pay fees.

other data controllers and data processors

Other data controllers and data processors currently are exempt from complying with the Act until 2nd June 2026.

Organisations should:

- evaluate the number of data subjects in Malawi whose personal data they currently process or intend to process;
- evaluate if they are processing or intend to process personal data of significance to the economy, society or security of Malawi;
- if they qualify as “of significant importance”:
 - comply with the Act;
 - register with the Authority and pay the required fees;
 - maintain up-to-date information with the Authority; and
 - inform the Authority in the future if there are changes.
- Other organisations have no registration requirements but must comply with the Act starting from 3rd June 2026

Data controllers and processors

s.2

Distinction between data controllers and data processors



Data controllers determine the purposes and means of the processing of personal data. Data processors process personal data on behalf of or at the direction of a data controller or another data processor.

Organisations should:

- assess whether they determine the purposes and means of the processing of personal data, in which case they are data controllers; and
- assess whether they process personal data on behalf of or at the direction of a data controller or another data processor; and
- review their obligations under the Data Protection Act accordingly.

s.32

Relationship between data controllers and data processors



The Data Protection Act requires data controllers and data processors to enter into a written agreement where the data controller or data processor intends to outsource the data processing to a data processor.

A data controller and a data processor who intend to process personal data of a data subject shall:

- enter into a written agreement
- ensure that the written agreement sets out:
 - the subject matter and duration of the processing of the data;
 - the nature and purpose of the processing of the data;
 - the type of data and categories of data subjects;
 - the rights and duties of the data controller and data processor;
- ensure that a data processor does not engage another data processor without the prior written authorization of the data controller.

s.8,
s.27,
s.28,
s.29,
s.30,
s.33,
s.35,
s.36,
s.37,
s.38

Responsibilities and Duties of data controllers and data processors

Under the Data Protection Act, data controllers and data processors have a duty to:

- adhere to the principles relating to processing of personal data prescribed under the Act (s 8 & 27);
- implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data (s 28 & 35);
- respect the rights of data subjects prescribed under the Act (s 19 - 25);
- maintain, in writing, a record of each personal data processing activity (s 29);
- conduct a data protection impact assessment where the processing of personal data is likely to be of high risk to the rights and freedoms of a data subject by virtue of the nature of the data, the scope, context and purpose of the processing (s 30);
- designate a suitably qualified person as a data protection officer where:
 - the data processing is carried out by a public authority;
 - the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of data subjects on a large scale; or

Organisations should:

- assess their roles and review their obligations under the Data Protection Act;
- Implement the required technical and organisational measures;
- establish lines of communication between data controllers and data processors to enable rapid, clear flow of information and assistance to ensure compliance with the Act;
- put in place mechanisms that will ensure the respect of the rights of data subjects;
- establish a record keeping system of each data processing activity;
- conduct a data protection impact assessment where the processing of personal data is likely to be of high risk to the rights and freedoms of a data subject by virtue of the nature of the data, the scope, context and purpose of the processing;
- designate a suitably qualified person as a data protection officer;
- verify age and consent of children and others lacking legal capacity;
- establish record keeping systems for personal data breaches; and
- where data is to be transferred outside of Malawi, review the basis for the transfer and ensure compliance.

- the core activities of the data controller or data processor consist of processing, on a large scale, sensitive personal data, pursuant to section 16 or personal data relating to criminal offences and convictions pursuant to section 18, designate a suitably qualified person as a data protection officer
- implement appropriate technical and organisational measures to ensure the security of personal data under the control or possession of the data controller or data processor, taking into account:
 - the cost of technology;
 - the nature, scope, context and purpose of processing personal data;
 - the degree and likelihood of harm to a data subject that could result from the loss, disclosure or other misuse of personal data; and
 - the retention period of personal data.
- verify age and consent of children and others lacking legal capacity (s 17);
- notify the Authority, in the case of breach of personal data, within 72 hours of becoming aware of the breach (s 36(1));
- notify a data subject, where there is a personal data breach which is of high risk to rights and freedoms of a data subject, of the breach, within 72 hours of the data controller becoming aware of the breach (s 37);
- keep a record of data protection breaches (s 36(4)); and

- not transfer personal data from Malawi to another country or an international organization, without legal basis and the authority's approval (s 38 & 39).

Compliance with data protection principles

s.8,
s.16,
s.18

Reviewing data processing activities

Compliance with the Act will require proactive efforts to understand what personal data an organisation processes and to bring its processing into line with the Act.

Organisations should:

- map out their current processing activities and types of personal data they process;
- consider whether the organisation's data processing complies with the Act by working through a checklist and recording whether the requirements apply and how they are met.

s.8,
s.16,
s.17,
s.18

Establishing lawful basis of processing

The Data Protection Act requires controllers to have a lawful basis to process personal data. Personal data relating to children (s 17) attracts particular restrictions.

Both data controllers and data processors must comply with additional requirements before processing sensitive personal data.

“Sensitive personal data” includes biometric data, race or ethnic origin, religious or other beliefs relating to the freedom of conscience of the person, health status, political opinion or affiliation, or such other data the Minister may prescribe.

Organisations should:

- establish what is the basis for lawful processing of personal data (or stop processing it where there is no lawful basis), such as:
 - consent of the data subject;
 - necessity to protect vital interests of a data subject or another natural person;
 - necessity to enter into or perform a contract;
 - legal requirement or obligation;
 - authorisation by law and mandate for a public authority;
 - a task in the public interest or exercise of official authority;
 - requirement of a court order or law; or
 - necessity for purpose of legitimate interests; and
- identify any “sensitive personal data” and ensure that the processing of such data meets any one of the following requirements under section 16 of the Act:
 - consent of the data subject
 - necessity to protect the interest of the data subject;
 - necessity to the exercise or performance of a right or obligation under a written law or court order
 - the processing of the data is in the interest of public health;
 - the processing of the data is for public interest;
 - necessity to the establishment, exercise or defence of a legal claim, obtaining legal advice or conduct of a legal proceeding;
 - the processing of the data is necessary 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; or
 - 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 aim and the data processing is carried out in the course of implementing a legitimate activity of the data controller or data processor to its members or former members or to a natural person who is in regular contact with the data controller or data processor, in connection with its purposes; and

s. 14

Demonstrating consent



Where they rely on a data subject's consent for anything, data controllers are responsible for demonstrating that they have obtained such consent, including from the parent or legal guardian of a child.

Consent must be specific, informed and unambiguous agreement or approval by a natural person, given freely, in writing, orally or by any affirmative action, to a data controller or data processor to process personal data relating to that person or to another natural person on whose behalf the person has the authority to provide the consent;

- identify any personal data relating to children or other individuals lacking legal capacity to consent.

Organisations should:

- devise disclosures to data subjects prior to obtaining consent, and establish mechanisms for obtaining data subject consent that qualify under the Act;
- avoid bundling consent for multiple purposes of processing;
- In processing personal data of children under 18 and others lacking legal capacity, ensure they obtain necessary documents to verify age and consent and status of parent or other legal guardian;
- review how they record consent and consider how to keep a clear record of what each individual data subject consented to;
- where consent is made a condition of receipt of a service, either document the justification (e.g., that it is necessary for the performance of the contract) or document a sufficient incentive to justify such conditionality (e.g., that a cheaper service is being provided in exchange for the consent);
- inform the data subject that he/she can withdraw consent, and ensure that it is as easy for the data subject to withdraw consent as to provide it ; and
- generally be cautious in relying on consent, recognising its limitations as a meaningful justification of processing.

s.9,
s.10,
s.11

Specifying purpose of data processing, minimization and accuracy



Personal data should be collected and processed for specific and legitimate purposes. The Act also applies certain standards relating to the adequacy, relevance and accuracy of personal data.

Organisations should:

- review and document the purposes for which they collect and further process personal data, and ensure that they do not exceed such purposes;
- establish processes to ensure that personal data collected is adequate, relevant and limited to the minimum necessary for such purposes; and
- take steps to ensure that personal data collected is accurate, complete, not misleading and, where necessary, kept up to date.

s.12

Data storage



Personal data should be retained for no longer than is necessary to achieve the purpose for which the personal data was collected or further processed except where required or authorised by law or the data subject has consented.

Organisations should:

- review or put in place internal data protection policies / guidelines covering records management programme with maximum storage periods for personal data categories, as well as minimum retention periods.
- Minimum retention periods will be informed by industry standards (e.g financial sector, 7 years)

s.30

Data protection impact assessment (DPIA)



Where the processing of personal data is likely to be of high risk to the rights and freedoms of a data subject by virtue of the nature of the data and the scope, context and purpose of the processing, a data controller shall, prior to the processing, carry out a data protection impact assessment.

A data controller must submit the DPIA report to the Authority prior to the processing of the personal data.

Specifically, a DPIA will be required where:

- personal data will be processed using an automated processing system including profiling;
- sensitive personal data, or personal data relating to a criminal offence or conviction, will be processed on a large scale; or
- there will be systematic monitoring of publicly accessible area on a large scale.

Organisations should:

- before commencing personal data processing, consider whether there is a high risk to the rights and freedoms of data subjects and whether a DPIA is required;
- if they conclude that no DPIA is required, make a written record of this decision and reasons for it;
- if it is determined that a DPIA is required, ensure that there is a clear process for carrying out a DPIA appropriately across the organisation, including preparing:
 - a systematic description of the envisaged personal data processing and its purpose;
 - an assessment of the necessity and proportionality of the processing in relation to the purposes for which the personal data would be processed;
 - where applicable, the legitimate interest pursued by the data controller, data processor or third party, as the case may be;
 - an assessment of the risks to the rights and freedoms of data subjects; and
 - the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance.

Data subjects

s.15

Disclosures to data subjects at the time of collecting the personal data

A data controller who collects personal data from a data subject shall, at the time of collecting the data, provide the following information to the data subject:

- the identity and contact details of the data controller or representative of the data controller;
- the legal basis for processing the personal data;
- the purpose for processing the personal data;
- where possible, the storage period for the personal data;
- the existence of automated decision-making, including profiling;
- the rights of the data subject provided under Part IV;
- the right to lodge a complaint with the authority under section 44; and
- whether the data controller intends to transfer the personal data to a place outside Malawi.

Organisations should:

- prepare written disclosures that are readily understandable and placed in a relevant manner to attract attention.

s.26,
s.27,
s.28,
s.29,
s.30

Honouring the rights of data subject

The Act establishes various data subject rights that they may exert against data controllers.

These include the right to:

- access their personal data (s 19)
- data portability (s 20)
- rectification (s 21)
- erasure (s 22)
- restriction of processing (s 23)
- object (s 24)
- not to be subject to automated decision making.

Organisations should review or put in place:

- internal data protection policies and procedures covering responses to data subject requests, i.e., data subject access to personal data relating to them, correction, deletion, right to object to certain types of processing and right not to be subject to a decision based solely on automated processing of personal data;
- external privacy policy describing the purpose for which and how personal data relating to data subjects is processed;
- where applicable:
 - customer marketing protocols and consent management where consent is the basis of processing personal data;
 - supplier and business partner notices and consents;
- data portability mechanisms

Organisations should:

- assess when data subject rights apply, and how they will be exercised
- consider how to organise and search for, filter and separate the information required to comply with the requests;
- consider whether the rights can be met wholly or partially through a self-service option;
- identify the relevant exemptions under the Act (e.g., in areas of national security, defence, prevention / detection of crimes, public security or public interest) and how the rights can be limited ; and
- ensure that mechanisms are in place to provide responses within a reasonable time.

Data security

s.35

Measures for protecting data



Data controllers and data processors must implement appropriate technical and organizational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control, including protections against accidental or unlawful destruction, loss, misuse or alteration, unauthorized disclosure or access.

Organisations should:

- consider carefully what security measures would be appropriate, taking into account:
 - the nature, scope, context and purpose of processing personal data;
 - potential harm to data subjects from the loss, disclosure or other misuse of the personal data;
 - the extent of the processing and period of data retention; and
 - the relative cost of any technologies, tools or other measures to be implemented;
- consider whether any of the following measures would be appropriate:
 - pseudonymization or other methods of de-identification;
 - encryption;
 - processes to ensure security, integrity, confidentiality, availability and resilience of processing systems and services;
 - data restoration processes, in case of an incident;
 - periodic risk assessments;
 - regular testing, assessing and evaluation of the measures implemented against the risks; and
 - regular updating of the measures and introduction of new measures;

s.36,
s.37



Notification of personal data breaches

Data controllers and data processors have obligations when a data breach occurs. Data processors are obligated to inform data controllers of any breach as stipulated in a contract between the data controller and the data processor. Data controllers must notify the Authority of the breach within 72 hours after becoming aware of it. Where there is a personal data breach of high risk to the rights and freedoms of a data subject, the data controller must notify the data subject of the breach within 72 hours of becoming aware of the breach.

Organisations should:

- set up data breach response and notification procedures to meet 72-hour deadlines for notifications from data processors to controllers, and from controllers to the Authority;
- put in place data breach response procedures to evaluate situations exposing data subjects to “high risk” and procedures to enable notifications to be made to data subjects within 72 hours;
- ensure that data processor agreements have provisions to enable data controllers to meet the 72-hour deadlines for reporting breaches to the Authority and that liability is understood;
- prepare template letters with the required information for notifications under section 36 (2) of the Act;
- conduct drills in respect of data breaches;
- maintain a record of personal data breaches, including at least the facts relating to any personal data breach, its effects and the remedial action taken to allow the Authority to verify compliance; and
- consider the adequacy of insurance coverage for data breaches given the level of fines and penalties under the Act and risk of complaint / action by data subjects.

Transferring personal data abroad

s.38,
s.39

Cross-border data transfers

The Act restricts the transfer of personal data abroad without adequate protections. The Authority may designate a country, region or specified sector within a country, or standard contractual clauses (SCCs) as affording or as not affording an adequate level of protection. The absence of such a determination, however, does not imply the adequacy or inadequacy of these. If the Authority has not made such a determination, data controllers should therefore assess adequacy for themselves. Personal data should not be transferred abroad before the Authority has made a determination that the destination country or the international organization or the recipient of the personal data outside Malawi will provide an adequate level of protection to the personal data.

Organisations should:

- review and map any flow of personal data outside Malawi, including:
 - within the organisation's Group; and
 - outside the organisation's Group;
- identify the countries to which the personal data is being transferred;
- consider what basis permits such transfer, including:
 - existence of an adequate data protection law in the destination country;
 - use of binding corporate rules (BCRs) by the organisation's Group;
 - adequate standard contractual clauses (SCCs) between transferor and transferee;
 - adherence to a code of conduct or certification mechanism;
 - consent of the data subject;
 - necessity of the transfer for contracting with the data subject; or
 - transfer for the benefit of the data subject where consent cannot be obtained;
- verify whether the Authority has made any designation of adequacy of a law, country, region, sector or SCCs;
- if not, then document conclusions as to adequacy of the protections of law, BCRs, SCCs or code of conduct or certification mechanism;
- consider whether BCRs would be a viable option for intra-group data transfers; and
- ensure that the obligations to protect data transferred abroad are implemented throughout the outsourcing chains.

Organisational readiness

General

Establishing internal governance



The Act requires the organisations to implement measures to reduce the risk of non-compliance. They should be able to demonstrate that they take data protection seriously. Data protection requires significant prominence within organisations as well as board attention and support.

Organisations are advised to:

- educate their senior management about the requirements under the Data Protection Act and the possible impact of non-compliance;
- identify key senior stakeholders to support a data protection compliance programme;
- allocate responsibility and budget for data protection compliance;
- consider reporting lines within the data protection governance structure; and
- appoint or designate a Data Protection Officer (DPO) if they are a public body or data controller or processor of significant importance.

General

Training



Data controllers should ensure that they build capacity of their employees through regular trainings

Organisations are advised to:

- implement data protection training programs specifically relevant to their organisations; and
- implement a policy for determining when training should take place and when refresher training should be carried out as well as a process for recording when training has been completed.