

Malawi Communications Regulatory Authority

Guidelines and Checklist on Compliance with the Data Protection Act [2022]

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
Scope and entry into force.....	1
Personal data and data processing	1
Geographic scope.....	2
Two-year grace period for most data controllers and processors	2
Immediate application to data controllers and processors of major importance	3
Data controllers and processors	4
Distinction between data controllers and data processors	4
Engaging data processors	4
Responsibilities of data processors	5
Compliance with data protection principles.....	6
Reviewing data processing activities.....	6
Establishing lawful basis of processing.....	6
Demonstrating consent.....	7
Specifying purpose of processing and minimising it.....	7
Retaining data	8
Data protection impact assessment (DPIA)	8
Data subjects.....	9
Making necessary disclosures to data subjects.....	9
Honouring data subject rights	10
Employee data.....	11
Customer, client, patient and supplier data	11
Data security	12
Measures for protecting data	12
Notification of personal data breaches	13
Transferring personal data abroad.....	14
Lawful basis for exporting personal data	14
Organisational readiness	15
Establishing internal governance	15
Training	15

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 (referred to herein as the Authority) is mandated by the new Data Protection Act, [2022] (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 will require companies, business partnerships and other private sector organisations, ministries, departments and agencies of central and local government, 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, and this Guideline also serves to educate the population. This both secures their individual rights and acts as a discipline on the conduct of organisations to improve the general standard of data governance.

The Act brings Malawi into a fast lane of digital development, providing an essential pillar that safeguards against risks and enables the country to move forward embracing the opportunities of the digital economy.

Organisations in Malawi and those outside that target people in Malawi are subject to the new framework. The Act positions Malawi to develop its information technology sector, inviting those needing to outsource their data processing to trust that Malawi's providers will protect their data. Robust penalties for noncompliance indicate the seriousness with which Malawi takes these responsibilities.






These Guidelines provide an overview of the requirements likely to affect most types of organisations. They should help organisations understand potential gaps they may have in compliance and the practical 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 within the next 12-months 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 Act enters into force with respect to these organisations upon entry into force. It provides a two-year grace period to all other Malawi data controllers and processors. It is likely that most organisations are not currently compliant with its requirements, and so all organisations should prepare to assess their compliance and to take steps to align with its provisions.

The Act repeals and replaces data protection provisions that were included in Part VII of the Electronic Transactions and Cybersecurity Act, 2016 [Chapter 74:02 of the Laws of Malawi].

The guideline and checklist below provide references to section numbers in the Act, summarises key requirements and provisions of the Act, and provides guidance and recommendations as to what should be done to comply. 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 

Scope and entry into force

s 3



Personal data and data processing

The Data Protection Act applies to processing of personal data:

- Personal data is defined broadly as any information relating to an individual who can be identified or is identifiable, 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 individual; and
- Processing is also defined broadly to include any operation or set of operations which is performed on personal data, whether or not by automated means, such as
 - collection, recording, organisation and structuring, storage,
 - adaptation or alteration,
 - retrieval, consultation, use,
 - disclosure by transmission, dissemination or otherwise making available,
 - alignment or combination,
 - restriction, erasure or destruction.
- The Act does not apply to processing by individuals solely for personal, recreational or household purposes.

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, whether they are processing personal data.

s 4

Geographic scope



The Data Protection Act applies where:

- the data controller or data processor is domiciled, ordinarily resident, or ordinarily operating in Malawi;
- the processing occurs within Malawi (other than mere transiting of data through Malawi); or
- the processing relates to the targeted offering of goods or services to the data subject in Malawi, or the monitoring of the behaviour of the data subject as far as his behaviour takes place within Malawi.

Organisations should:

- verify where they are domiciled, ordinarily resident or ordinarily operating;
- verify whether they are monitoring or targeting data subjects in Malawi;
- verify also whether data processors that are 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 it and personal data processing it conducts complies with this Act.

s 5

Two-year grace period for most data controllers and processors



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.

Organisations should:

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

ss 3, 5,
6(2)(o),
37, 38

Immediate application to data controllers and processors of major importance



The Data Protection Act applies immediately to data controllers or data processors (see below) 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. They must register with the Authority and pay fees.

The Authority has the power to raise the 10,000 threshold, and also to add other classes of data controller or data processor that process personal data of particular value or significance to the economy, society or security of Malawi.

Organisations should:

- evaluate the number of data subjects in Malawi whose personal data they currently process or intend to process;
- if they qualify as “of major importance”:
 - urgently prepare compliance 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 they no longer qualify.

Data controllers and processors

s 3

Distinction between data controllers and data processors



Data controllers determine the purposes and means of the processing of personal data. Data controllers have extensive obligations under the Data Protection Act towards data subjects and the Authority. 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 25

Engaging data processors



The Data Protection Act makes data controllers and processors responsible for ensuring compliance when they outsource or delegate data processing to third party data processors.

Organisations should:

- check what organisations they outsource processing of personal data to;
- review the security, integrity and confidentiality of personal data that is processed by such third parties;
- implement appropriate technical measures (e.g., encryption) and organisational measures (e.g., limiting access to those specifically authorised) to protect these;
- establish information exchange protocols to ensure compliance; and
- enter into a written agreement for the outsourced data processing.

ss 3,
20(2),
25, 31,
34, 36

Responsibilities of data processors

Despite being contractors often having no relationship with the data subject, data processors have direct obligations under the Data Protection Act to:

- implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data;
- assist the data controller or any data processor that engaged it in fulfilling the data controller's obligations to honour data subjects' rights;
- provide the data controller or any data processor that engaged it with any information it reasonably requires to demonstrate compliance with the Data Protection Act;
- notify the data controller or any data processor that engaged it when any new data processors are engaged;
- ensure that any sub data processor it engages will comply with the data protection principles applying to the data controller;
- verify age and consent of children and others lacking legal capacity;
- notify the data controller or any data processor that engaged it of any personal data breach within 72 hours and provide information about the breach;
- keep a record of data protection breaches; and
- not transfer personal data outside Malawi without legal basis for doing so.

Organisations should:

- assess their roles and, if they qualify as data processors, review their obligations under the Data Protection Act;
- understand the obligations of data controllers which they ultimately serve;
- take the required technical and organisational measures;
- establish lines of communication with data controllers or data processors that engage them to enable rapid, clear flow of information and assistance with compliance when required;
- establish standards for their procurement of services from sub-processors to ensure their compliance and include minimum terms in their agreements;
- establish record keeping systems for data protection breaches; and
- review where data is to be transferred abroad and ensure compliance.

Compliance with data protection principles

ss 2,
18, 19

Reviewing data processing activities



Compliance with the Data Protection 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 Data Protection Act by working through a version of a checklist like this, and recording whether the requirements apply and how they are met.

ss 2,
18, 19,
20

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 (under 18) 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 similar beliefs (such as those reflecting conscience or philosophy), health status, sex life or sexual orientation, political opinions or affiliations, or anything else the Authority prescribes.

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 enter into or perform a contract or comply with a legal obligation;
 - authorisation by law and mandate for a public authority or a task in the public interest or exercise of official authority;
 - requirement of court order or law;
 - implementation of specific economic development or humanitarian initiative;
 - necessity for purpose of legitimate interests;
 - necessity of compliance with Access to Information Act; or
 - necessity for archiving in the public interest or historical, statistical or scientific research; and
- identify any “sensitive personal data” and establish the basis of lawful processing under section 19 of the Data Protection Act (or stop processing it); and
- identify any personal data relating to children or other individuals lacking legal capacity to consent.

ss
18(1),
19(1),
21,
23(c),
27,
29(c),
36(a) &
(d)



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 freely given, specific, informed, and unambiguous indication, whether by a written or oral statement or an affirmative action, of an individual's agreement to the processing of personal data relating to him or to another individual on whose behalf he has the authority to provide such consent.

Organisations should:

- review how they record consent and consider how to keep a clear record of what each individual data subject consented to;
- devise disclosures to data subjects prior to obtaining consent, and establish mechanisms for obtaining data subject consent that qualify under the Data Protection Act;
- avoid bundling consent for multiple purposes of processing;
- ensure they obtain necessary documents to verify age and consent and status of parent or other legal guardian in the case of processing personal data of children under 18 and others lacking legal capacity;
- where processing relies on consent and 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 (e.g., using a self-service dashboard); and
- generally be cautious in relying on consent, recognising its limitations as a meaningful justification of processing, so that consent may be better relied upon only when it is the only way to justify processing.

s 23



Specifying purpose of processing and minimising it

Personal data should be collected and processed for specified, explicit and legitimate purposes. The Data Protection 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.

ss 23

Retaining data



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.

ss 24

Data protection impact assessment (DPIA)



Two years after the Data Protection Act enters into force, data controllers will be required to carry out a DPIA before carrying out processing that is likely to result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context and purposes. A data controller must submit the data impact assessment report to the Authority before the processing begins. If there is a high risk to the rights and freedoms of the data subject, the data controller should consult the Authority before the processing operations.

Organisations should:

- before commencing personal data processing, consider whether there is a high risk to rights and freedoms of data subjects and so 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 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;
 - 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

ss 22

Making necessary disclosures to data subjects



Data controllers are required to inform data subjects from whom they directly collect personal data of the identity and contact information for the data controller, basis of processing, sharing of the data with third parties, data subject rights and right to lodge a complaint to the Authority.

Organisations should:

- identify where disclosures should be made to data subjects; and
- prepare written disclosures that are readily understandable and placed in a relevant manner to attract attention.

ss 26,
27, 28,
29, 30

Honouring data subject rights

The Data Protection Act establishes various data subject rights that they may exert against data controllers. These include the right to:

- confirmation as to whether or not the data controller, or a data processor operating on its behalf, is processing personal data relating to the data subject and the source of such personal data;
- a copy of such personal data in a commonly used electronic format (subject to a contribution to the costs);
- correction or otherwise deletion of personal data that is inaccurate, out of date, incomplete or misleading; and
- deletion of personal data which the data controller is not entitled to retain;
- withdraw previously provided consent to processing; and
- not be subject to automated decision making.

Organisations should review or put in place internal data protection policies / guidelines covering:

- responding to data subject rights, i.e., data subject access to personal data relating to them, correction, deletion, right to object to certain types of processing and right to object to or obtain human intervention in certain automated decision making;
- external privacy policy describing the purpose for which and how personal data relating to customers is processed;
- customer marketing protocols and consent management where consent is the basis of processing personal data;
- supplier and business partner notices and consents; and
- data portability (if the Authority establishes such rights under section 30).

Organisations should:

- assess when data subject rights apply, and how they will be exercised in the context of customers, clients, patients and employees;
- consider how to organise and search for, filter and separate the information required to comply with the rights;
- consider whether the rights can be met wholly or partially through a self-service option;
- identify the relevant exemptions under the Data Protection Act (e.g., in areas of national security, defence, prevention / detection of crimes, public security or public interest) and how the rights can be resisted where desirable;
- ensure that mechanisms are in place to provide responses within a reasonable time; and
- assess the opportunities to have personal data of competitors or other third parties' customers ported to the organisation through data subject's exercise of portability rights (if the Authority establishes such rights under section 30).

General **Employee data**



Organisations are advised to review or put in place internal data protection policies and guidelines covering:

- HR department handling of employee data;
- a notice provided to employees of all data collected and for what purpose (both employee, customer and other third parties);
- general handling of other employees' personal data and customer personal data by all employees;
- monitoring of employee communication and internet usage, including through 'bring your own device' (BYOD) solutions and social media;
- accessing employee files / communications for investigations; and
- electronic monitoring of employee location and conduct.

General **Customer, client, patient and supplier data**



Organisations are advised to review or put in place internal data protection policies / guidelines covering:

- external privacy policy describing the purpose for which and how personal data relating to customers, clients and patients is processed;
- customer marketing protocols and consent management where consent is the basis of processing personal data; and
- supplier and business partner notices and consents.

Data security

ss 31 &
32

Measures for protecting data



Data controllers and 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;
- take into account the following when considering measures:
 - the amount and sensitivity of the 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;
- when considering what measures to employ, take into account:
 - available technologies and systems;
 - the cost of implementing the security measures; and
 - the relative risks and likely harms to the rights and freedoms of the data subjects.

Notification of personal data breaches



Data controllers and processors have obligations when a data breach occurs. These flow up the chain with a view to ensuring that the data controller can notify the Authority and data subjects concerned when required. Data processors are obligated to inform data controllers of any breach within 72 hours of becoming aware of it. Data controllers must notify the Authority of the breach within 72 hours after becoming aware of it if the breach is likely to result in a risk to the rights and freedoms of individuals. If that risk is high, then the data controller must communicate the breach to the data subject without undue delay as well.

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 “without undue delay” in such circumstances;
- 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 33(4) of the Data Protection Act;
- conduct rehearsals 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 Data Protection Act and risk of complaint / action by data subjects.

Transferring personal data abroad

ss 35 &
36

Lawful basis for exporting personal data



The Data Protection 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.

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 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 by the organisation's group (BCRs);
 - adequate 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 obligations to protect data transferred abroad are implemented down through outsourcing chains.

Organisational readiness

General

Establishing internal governance



The Data Protection Act's requirements will depend on organisations implementing measures to reduce the risk of non-compliance with the Act. They should be able to demonstrate that they take data protection seriously. Data protection requires significant prominence within organisations as well as attention and support of the board of directors.

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; and
- consider reporting lines within the data protection governance structure.

General

Training



It is next to impossible to demonstrate that an organisation is able to achieve compliance without policies setting out how to comply coupled with training to bring those policies to life.

Organisations are advised to:

- implement a training programme covering data protection generally and the areas that are 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.