MALAWI

Cross-Border Sharing of Data

This section reviews the rules as required by data protection law in the cross-border sharing of personal data. The rules on the cross-border sharing of personal data under data protection law do not exist in a vacuum, and therefore other important information that must be followed when sharing personal data is discussed. This information, however, is comprehensive as it relates to the cross-border sharing of personal data.

The relevant national health research regulations as they relate to the cross-border sharing of personal data are reviewed. These national health research regulations set out the required legal and ethical conditions that must be met when processing personal data for research. Applicable national legal and ethical documents are listed, but the discussion only specifies the requirements as they relate to the cross-border sharing of personal data for research. The guide does not treat the legal and ethical requirements generally required for research, and therefore users of this guide must consult with these documents to ascertain these requirements and to ensure that they are met.

An overview of the data protection law is provided. This includes what data the law applies to, the categories of data, the key individuals in the Bill, the key principles required to be met in the processing of personal data, and the rights of data subjects. This is an overview only to help users to understand *some* of the requirements of the Bill and to begin to assist users in navigating the Bill. It is not comprehensive, and users of this Bill must consult it to understand all relevant and applicable requirements to be met, and to understand any exceptions that may be in place for research. This is necessary as all these requirements must be met in the processing of personal data for research, in addition to the requirements on cross-border sharing of data.

The section provides users with a comprehensive description of the requirements to be met in the cross-border sharing of personal data for research. It sets out all the necessary conditions that must be met to legally share data across borders for research.

In countries where no data protection law is in force, the necessary national legal and ethical requirements, as they relate to the cross-border sharing of data, are presented.

The cross-border sharing of data is governed by several legal and ethical regulations, all of which must be met prior to the sharing of data for research. In Malawi, the Data Protection Act, 2024, is in force. It is a general data protection law that applies to the processing (i.e., use) of personal data in all sectors. While it is not a statute introduced specifically to regulate research, it applies to

research that involves the processing of personal data. It is only one of several laws that must be complied with when transferring personal data for research purposes.

Health Research Regulations and Cross-Border Data Sharing

In addition to the national laws listed below, several international treaties and conventions have been signed. Of importance in this domain is the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) that recently came into force. Malawi has not ratified the Malabo Convention.

The relevant national legislation and guidance are:

- Constitution of Malawi
- Data Protection Act
- Public Health Act
- Science and Technology Act, which mentions research
- National Health Research Agenda, 2012
- National Policy Measures and Requirements for the Improvement of Health Research Co-ordination in Malawi, 2012. This was published by the National Commission for Science and Technology and relates to Malawi's Science and Technology Act.
- Policy Requirements, Procedures and Guidelines for the Conduct and Review of Human Genetic Research in Malawi, 2012

These documents set out the legal and ethical requirements that must be met for the conduct of research in Malawi. Malawi has strict provisions on the use of genetic material and data in research. Transfer of genetic material (locally or nationally) can take place only if the researcher and the other research group are collaborating on a research study that has been approved by the National Health Sciences Research Committee (NHSRC), if genetic material and information is provided in a form that ensures that participants cannot be identified, and the research group ensures that privacy and confidentiality are not compromised while holding the material and information.

Cross-border movement of genetic material is not permitted unless there is a justifiable reason to do so, such as to expedite a timely therapeutic cause. In such a case, cross-border movement of genetic material is not permitted unless prior approval for such a transfer under a material transfer agreement has been reviewed and signed by the NHSRC. To transfer genetic material, the NHSRC must approve the research study. The application must describe how privacy and confidentiality of the individuals and communities, as well as safety of such materials, will be maintained.

Data Protection Act

In addition to these legal and ethical requirements, the Data Protection Act applies to the processing of all personal data, but owing to the importance of research, there are special provisions in place for this. Personal data may be processed for inter alia scientific research, and sensitive personal data may be processed for scientific research, but only if one of the conditions for the processing of personal data in the Data Protection Act has been met – one of which is for research. The conditions set out in the Data Protection Act must all be met for research. In addition, extra conditions must be met prior to the transfer of personal data across borders.

Some of the techno-legal terms used in the Data Protection Act are discussed below. This is not a thorough assessment of the Act as it applies to research, but rather an overview of some of the key terms and conditions that must be met in the processing of personal data for research.

The Main Actors Defined in the Data Protection Act

	Legal definition	**Layman explanation**
Data subject	A natural person to whom particular personal data relates.	The person to whom the data relates.
Data controller	A natural or legal person who, alone or jointly with another natural or legal person, determines the purpose and means of processing personal data.	The person who decides what the data will be used for in research. Legal responsibility falls on the Principal Investigator (PI) *and* on the research institution (as employer).

Data controller of significant importance	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 10 000 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.	
Data processor	A natural or legal person who processes personal data on behalf of a data controller.	Someone who is not directly employed by the data controller, but who processes personal data under the direction of the data controller. They may be a consultant, for example.
Data processor of significant importance	A data processor who – (a) is domiciled, ordinarily resident, or ordinarily operates in Malawi and processes or intends to process personal data of more than 10 000 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.	
Regulator	Not defined in the Data Protection Act, but the Malawi Communication Regulatory	The independent body tasked with monitoring and enforcing compliance with the law.

	Authority is designated as the Data Protection Authority.	
Data Protection Officer	A person designated as such by the Act.	An individual in an organisation who is appointed to advise and promote compliance with the law.
Third party	A natural or legal person other than a data subject, data controller or processor, who is authorised to process personal data under the direct authority of a data controller or data processor.	
Authority	The Malawi Communications Regulatory Authority established under the Communications Act.	

Categories of Data Listed in the Data Protection Act

	Legal definition	**Layman explanation**
Biometric data	Personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a natural person which confirms the unique identification of that person, and includes a physical measurement, facial image, blood type, fingerprint, retinal scan, voice recognition and deoxyribonucleic acid analysis.	Physical or behavioural characteristics like fingerprints or facial recognition, used to identify individuals.

Personal data	Any data relating to an identifiable natural person which, directly or indirectly, refers 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.	Data/information about a particular person that can identify him or her.
Sensitive personal data	Personal data relating to a natural person's – (a) biometric data; (b) race or ethnic origin; (c) religious or other beliefs relating to the freedom of conscience of the person; (d) health status; (e) political opinion or affiliation; and (f) such other data as the Minister may prescribe.	Personal data/information about a particular person which is considered sensitive, such as health data and genetic data, and which receives additional legal protection.
Pseudonymisation	The processing of personal data in such a manner that the data cannot be attributed to a particular natural person without the use of additional information.	

While data protection law does not usually apply to anonymised data, the Data Protection Act does not explicitly exclude anonymised data from the ambit of its provisions. The Data Protection Act

clearly applies only to the processing of personal data, and therefore data which has truly been rendered no longer individually identifiable—i.e., anonymised—will presumably fall outside its ambit.

To determine whether data to be shared is anonymised, it is important to make an assessment, which can be challenging. There is no guidance from the Regulator on this point, but the data controller may wish to follow the guidance set out to be followed under the GDPR on how to make an assessment to determine whether data has been anonymised – including anonymisation techniques.

The test for anonymisation is always objective, but it can be interpreted in two ways: context-specific (relative approach) or context-agnostic (absolute approach).

Accordingly, the test for determining whether data is anonymised can be approached in two ways:

1. **Context-Agnostic Test**: Is there anyone in the world who can identify the data subject from the data? This test assesses whether any individual, regardless of context, could identify the data subject.
2. **Context-Specific Test**: Can a specific holder of the data identify the data subject from the data? This test evaluates whether the specific data recipient, given their context and resources, can identify the data subject.

The choice of approach affects the treatment of pseudonymised data. For example:

1. **Context-Agnostic Test**: If Data Controller A sends pseudonymised data to Data Controller B (with A retaining the means to identify individuals), the dataset is not considered anonymised.
2. **Context-Specific Test**: If Data Controller A sends pseudonymised data to Data Controller B, the dataset *might* be considered anonymised in the hands of Controller B. However, a test is necessary to determine if the dataset is indeed anonymised for Data Controller B.

The first test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B, the dataset would not be anonymous.

The second test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B, the dataset *may* be anonymous in the hands of Data Controller B. A test would be needed to determine whether the dataset is anonymous in the hands of Data Controller B.

In the absence of direction from the Regulator on a test, the data controller will have to decide. In making this decision, general points may be worth keeping in mind (many of which come from guidance related to anonymisation under the GDPR):

- An assessment must be made on a case-by-case basis, considering the particular context.
- The anonymisation must be irreversible.
- The assessment is made on the current state of the art. As technology progresses, data that was once deemed to be anonymous may become personal data and therefore fall under data protection regulations.
- Consider all means of identification that could be used by a person, for example, available datasets.
- Consider objective factors that are *reasonably likely* to be used, such as technology, resources and time, to identify.
- One could follow the GDPR test which states that if an individual cannot be singled out, or identifiers cannot be linked to make a person identifiable, or it is impossible to infer a link between two pieces of information in a dataset, then the data is anonymous.
- Genetic data is considered sensitive personal data. It not only falls under the Data Protection Act but also has a higher level of protection.
- There is ongoing debate about whether genomic datasets can ever be rendered truly anonymised, particularly as genetic data is an identifier. In considering whether a genomic dataset can be considered anonymised, context matters – the objective factors associated with the data.

Key Principles That Must be Met in Terms of the Data Protection Act

1. *Lawfulness of data processing:* Personal data must be processed lawfully, fairly, and transparently in relation to the data subject. The processing of sensitive personal data is generally not permitted unless it falls within one of the grounds in the Data Protection Act.
2. *Provision of information:* When collecting personal data directly from a data subject, the data controller must provide the data subject with the identity and contact details of the data controller, the basis of processing and the purposes for which the processing of personal data is intended, information on the third parties which the data will be shared with, the rights of the data subject, and the right to lodge a complaint with the Authority. When personal data is not collected directly from the data subject, the data controller must abide by the provisions in the Data Protection Act, unless the data subject already has such information or providing such information is impossible or would involve a disproportionate effort or expense.
3. *Purpose limitation:* Personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
4. *Data minimisation:* Only the data that is necessary for the specific purpose should be collected and processed. It is essential that the personal data is adequate, relevant, and limited only to the amount of data that is required to achieve the objectives for the collecting or further processing of the personal data.
5. *Storage limitation:* Personal data should not be retained for longer than is necessary to achieve the purpose of processing. Where personal data is stored for longer periods, the principle of data minimisation must be adhered to and the personal data must be pseudonymised, where necessary.
6. *Accuracy:* Personal data must be accurate and, where necessary, kept up to date in terms of the purpose for which the personal data was collected.
7. *Data integrity and data confidentiality:* Personal data should be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Both organisational and technical measures must be put in place to secure the data.

Data Subject Rights in Terms of the Data Protection Act

Data subjects have rights that the data controller must protect. These rights are the:

1. *Right to access:* The data subject has the right to obtain from a data controller or data processor, confirmation of whether personal data concerning the data subject is being processed by the data controller or data processor, and where that is the case, the right to access the personal data being processed. The data subject has the right to obtain a copy of the personal data being processed in a commonly used electronic format within 30 days of receipt of the request and, where practicable, at no expense to the data subject. The data subject also has the right to be provided with information relating to 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; and whether the data controller intends to transfer the personal data to a place outside Malawi.
2. *Right to rectification:* The data subject has the right to rectify any error in their personal data and the right to have incomplete personal data completed. A data controller or data processor who receives a request for rectification or supplementary data for completion by the data subject must rectify the error in the personal data or add the supplementary data to the personal data of the data subject within 14 days of receipt of the request or the supplementary data.
3. *Right to erasure:* The data subject has the right to have personal data erased, where the personal data is no longer necessary in relation to the purpose for which the data was processed; the data subject withdraws the consent for processing and there is no other legal ground for processing; the data subject objects to the processing of the personal data and there is no overriding legitimate ground for processing the data; the personal data has been unlawfully processed; or there is a legal obligation under a written law to erase the personal data.

4. *Right to object:* The data subject has the right to object to the processing of his/her personal data where the processing is causing, or is likely to cause, substantial damage or substantial distress to the data subject, and the damage or distress is, or would be, unwarranted. Upon receipt of the objection, a data controller or data processor must cease to process the personal data, unless the data controller or data processor demonstrates that there is a compelling legitimate ground for the processing which overrides the interest or right of the data subject, or the processing is necessary for the establishment, exercise or defence of a legal claim.
5. *Right to restrict processing of personal data:* The data subject has the right to restrict the processing of personal data where the accuracy of the data is contested by the data subject, or the data controller or data processor no longer needs the data for the intended purpose of processing. An exception is if the data controller or data processor shows cause, in writing, why the request cannot be adhered to.
6. *Rights in relation to automated decision-making and profiling:* The data subject has the right to object to a decision based solely on automated processing, including profiling, which produces a legal or similarly significant effect concerning the data subject. Exceptions are where the processing is necessary for entering into, or performance of, a contract between the data subject and a data controller; the processing is authorised by a written law which has suitable measures to safeguard the rights and interests of the data subject; or the processing is based on the consent of the data subject. Where an exception applies, a data controller must implement the appropriate measures to safeguard the rights and interests of the data subject.
7. *Right to data portability:* The data subject has the right to receive personal data about him/her from a data controller in a structured, commonly used and machine-readable format where the processing of the personal data is based on consent, fulfilment of a contractual obligation, or the processing is carried out by automated means. Upon request by the data subject, a data controller must provide the data subject with their personal data in a commonly used and machine-readable format, or transmit the data subject's personal data directly to another data controller specified in the request within 30 days of receipt of the request.

Cross-Border Transfer of Personal Data

When considering cross-border transfers of data for research, all the provisions of the Data Protection Act must be met. The Data Protection Act also has a number of provisions on cross-border transfers of personal data that, in addition to the other provisions, must be met.

Cross-border transfers of personal data are not explicitly defined in the Data Protection Act. However, it would occur when personal data is being sent from a data controller or data processor in Malawi to a data controller in another country. It *could* also include a situation where a researcher outside of Malawi accesses the personal data inside the country. It *could* also include putting data onto a cloud where the server is not hosted in the country. However, this is not yet settled law.

Grounds for the cross-border transfer of personal data

In addition to meeting the provisions set out in the law, there must be a ground under which the cross-border transfer of personal data can take place. These grounds are:

1. *Adequacy of protection:* Personal data cannot be transferred to a recipient in a third country or international organisations unless there is a similar level of protection as that provided by Malawi through:
    a. a law;
    b. a binding corporate rule;
    c. a personal data protection contractual clause;
    d. code of conduct; or
    e. a certification mechanism.

2. The Authority is responsible for this assessment and will take into consideration:
    (a) the availability of enforceable data subject rights and the availability of mechanisms for data subjects to enforce their rights through administrative or judicial processes;
    (b) respect for the rule of law and human rights and freedoms by the country;

(c) the existence of a legally binding instrument between the Authority and the relevant public authority in the country, addressing elements of adequacy of data protection;
(d) the prevailing policy on access to personal data by a public authority in the country;
(e) the existence of an effective data protection law in the country;
(f) the existence of a functionally independent and competent data protection or similar supervisory authority with adequate enforcement powers; and
(g) international commitment and conventions binding on the country, including its membership of a relevant multilateral or regional organisation.

The Authority may also decide whether an international organisation or a recipient of personal data outside Malawi provides an adequate level of protection of personal data based on comparable adequacy decisions made by a competent data protection authority in another country.

The Minister may give notice in the Gazette of any country, region, or specified sector in a country, or a standard personal data protection contractual clause that it has determined as affording an adequate level of protection. The Authority may approve binding corporate rules, codes of conduct, or certification mechanisms proposed to it by a data controller, where the Authority determines that they have adequate protection.

Researchers are therefore encouraged to first consult the Gazette to see whether the cross-border transfer of personal data could fall under this adequacy provision.

3. *Other bases for transfer of personal data:* Without adequacy, personal data can be transferred outside Malawi, only if the:
   a. data subject has consented to the transfer and has been informed of the possible risks of the transfer;
   b. processing is necessary for the performance of a contract to which the data subject is party or at the request of the data subject prior to entering into a contract;
   c. transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party; or

d. transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject, and if it were reasonably practicable to obtain such consent the data subject would likely give it.

Where a data controller or data processor adopts binding corporate rules, a code of conduct or certification mechanism pursuant to this act, the data controller or data processor must submit the adopted corporate rules, code of conduct or certification mechanism to the Authority.

A data controller and data processor must keep a record of the basis for the transfer of personal data from Malawi to another country or an international organisation.