TANZANIA

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 PDPA, 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 PDPA and to begin to assist users in navigating the PDPA. It is not comprehensive, and users of this Act 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 personal data is governed by several laws and regulations, which must be carefully considered and complied with before researchers share data for research purposes. In Tanzania, the Personal Data Protection Act 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 law 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 Involving Human Participants and Cross-Border Data Sharing

In addition to the national laws listed below, several international treaties and conventions have been signed. However, Tanzania has not yet ratified the African Union Convention on Cyber Security and Personal Data Protection ('the Malabo Convention').

The relevant national legislation is:

- Constitution of the United Republic of Tanzania
- Human DNA Regulations Act
- Tanzania Commission for Science and Technology Act
- Tanzania Food, Drugs and Cosmetics Act
- Tanzania National Scientific Research Council Act
- Tanzania National Scientific Research Council (Amendment) Act
- Guidelines of Ethics for Health Research In Tanzania

These laws and guidelines set out the legal and ethical requirements that must be met for the conduct of research in Tanzania and must be considered when effecting cross-border transfer of personal data. It is an offence to send samples for human DNA analysis abroad without the permission of the Office of the Regulator of Human DNA Services. Moreover, the National Institute for Medical Research (NIMR) must approve all research that involves foreign researchers or collaborators. A contract Agreement is recommended for all research involving external researchers.[1]

[1] para 8.9. http://www.cohred.org/wp-content/uploads/2011/05/ETHICS-GUIDELINE-2009.pdf

Personal Data Protection Act

In addition to these legal and ethical requirements, the Personal Data Protection Act applies to the processing of all personal data, with special provisions in place that deal with the processing of personal data for research purposes. Two regulations related to this Act are also important: Personal Data Protection (Personal Data Collection and Processing) Regulations and the Personal Data Protection (Complaints Settlement Procedures) Regulations.

For research, the Act exempts the requirement of prior written consent for processing of sensitive personal data if the processing is necessary for scientific research and the Commission has, by special guidelines, specified the circumstances under which such processing may be carried out. This means that the consent requirement is not applicable in relation to scientific research but a special guideline must be put in place describing the circumstances applicable.

Extra conditions must be met prior to the transfer of personal data across borders.

Techno-legal terms used in the Act are discussed below. This is not a thorough assessment of the Personal Data Protection 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 Personal Data Protection Act

	Legal definition	Layman explanation
Data subject	The subject of personal data which is processed under the Act.	The person to whom the data relates.
Data controller	A natural person, legal person or public body which alone or jointly with others determines the purpose and means of processing of personal data; and where the purpose and	The person who decides what the data will be used for in research. Legal responsibility falls on the PI *and* on the research institution (as employer).

	means of processing are determined by law, "data controller" is the natural person, legal person or public body designated as such by that law and it includes his/her representative.	
Data processor	A natural person, legal person or public body which processes personal data for and on behalf of the data controller and under the data controller's instruction, except for the persons who, under the direct authority of the data controller, are authorised to process the data, and it includes his/her representative.	Someone who is not directly employed by the data controller but who processes personal data under the direction of the data controller. He/she may be a consultant, for example.
Data Protection Commission		The independent body established to monitor and enforce compliance with the law
Data Protection Officer	An individual appointed by the data controller or data processor who is charged with ensuring compliance with the obligations provided for in the Act.	An individual in an organisation who is appointed to advise and promote compliance with the law.
Health professional	A person providing healthcare services and who is recognised as such by the relevant law.	
Director General	The Director General of the Commission, who is appointed under the Act.	

Recipient	A natural person, legal person, public body or any other person who receives personal data from a data controller.	

Categories of Data Listed in the Personal Data Protection Act

	Legal definition	**Layman explanation**
Personal data	Data about an identifiable person that is recorded in any form, including: (a) personal data relating to the race, national or ethnic origin, religion, age or marital status of the individual; (b) personal data relating to the education, medical, criminal or employment history; (c) any identifying number, symbol or other particular assigned to the individual; (d) the address, fingerprints or blood type of the individual; (e) the name of the individual appearing on personal data of another person relating to the individual or where the disclosure of the name itself would reveal personal data about the individual; (f) correspondence sent to a data controller by the data subject that is explicitly or implicitly private or confidential, and replies to such correspondence that would reveal the	Data about a particular person that can identify him or her.

	contents of the original correspondence and the views or opinions of any other person about the data subject.	
Sensitive personal data	Sensitive personal data includes: (a) genetic data, data related to children, offences, financial transactions of the individual, security measures or biometric data; (b) if they are processed for what they reveal, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade-union membership, gender, and data concerning health or information on sex life; and (c) any personal data otherwise considered under the laws of the country as presenting a major risk to the rights and interests of the data subject.	Personal data about a particular person that is sensitive, such as health data and genetic data, and which receives additional legal protection.
Genetic data	Any personal data stemming from a DNA analysis	Data that is derived from the analysis of human DNA.
Anonymous data	Not defined.	Data from which it is no longer possible to identify a person. It must be impossible to re-identify the person. Data protection law does not apply to anonymised data.

Data protection law applies only to personal data. This is data that refers to an identified or identifiable person. For data that does not come under the definition of personal data, data protection law does not apply. The Personal Data Protection Act applies to "the processing of personal data".

The Personal Data Protection Act does not mention anonymised data. However, it allows the data controller to use personal data for purposes other than for which it was collected where it is "in a form in which the data subject is not identified" and for statistical or research purposes – as long as it is not published in a form that could reasonably be expected to identify the data subject. The test in the Act is whether it may reasonably be expected that the data subject could be identified and so the context suggests that the Act is not referring to anonymisation but to something less absolute.

Although the Personal Data Protection (Personal Data Collection and Processing) Regulations mention anonymisation, it is not defined. Anonymisation may be used by data controllers or data processors to minimise their use or retention of data in an identifiable form where it is not necessary to do so. This is in line with the principles of proportionality, necessity, retention and the storage of personal data. The data controller or data processor must ensure that there is "*no possibility* of re-identification of anonymous personal data" and that this is properly tested. The inclusion of the phrase 'no possibility' and the requirement for this to be tested suggests that for data to be considered anonymised, the anonymisation must be proved through testing to be effective and absolute. Again, the Act does not mention pseudonymised data, but the term is used in the Regulations, although it is not defined. It is, however, clearly used as a safety measure that involves "storing identification keys separately".

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 Commissioner 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 Commissioner on a test, the data controller will have to decide. In making this decision, general points may be worth bearing 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, in particular 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 the Personal Data Protection Act

1. *Lawfulness, fairness, and transparency*: Personal data must be processed lawfully, fairly, and transparently in relation to the data subject. Lawful means that there must be a legal basis for the processing of the personal data. The processing of sensitive personal data is generally not permitted unless it falls within one of the grounds in the Act. There is a special provision on the processing of sensitive personal data. The provision states that written

consent of the data subject prior to processing sensitive data is not required where the processing is necessary for scientific research and the Commission has, by special guidelines, specified the circumstances under which such processing may be undertaken.

2. Personal data is collected for explicit, specified and legitimate purposes and is not further processed in a manner incompatible with those purposes (purpose limitation).
3. Personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation).
4. *Accuracy*: Personal data must be accurate and, where necessary, kept up to date, with every reasonable step taken to ensure that any inaccurate personal data is erased or rectified without delay.
5. *Storage limitation*: Personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Once the objective of the processing has been achieved, the data should be deleted. Data that is rendered anonymous does not fall under data protection law. However, to anonymise the data, there must still be a lawful basis to do so.
6. *Data subject rights*: Personal data should be processed in accordance with the rights of the data subject.
7. *Security*: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against any loss, destruction or damage, using appropriate technical or organisational measures.
8. *Cross-border transfer of data*: Personal data should not be transferred abroad contrary to the provisions of the law.

Data Subject Rights Under the Personal Data Protection Act

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

1. *Right to be informed*: The data subject has the right be informed that his/her data is being processed and about the purposes of that processing. The data subject is also entitled to be informed by the data controller of the logic involved in decision-making where the automatic

processing of personal data for evaluating matters relating to a data subject has constituted or is likely to constitute the sole basis for any decision significantly affecting the data subject.

2. *Right to prevent processing*: The data subject has the right to prevent or to suspend the processing of his/her personal data by a data controller if the processing is likely to cause substantial damage to him/her or to another person.
3. *Right to prevent processing of personal data for direct marketing purposes*: The data subject may require the data controller to stop processing his/her personal data for direct marketing or the processing of personal data for financial benefits.
4. *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 unless it falls in one of the three categories exempted in law including a data subject's explicit consent. The procedure for notification of a data subject where a decision which significantly affects the data subject, is based solely on the processing by automatic means in the Regulations.
5. *Right to compensation*: The data subject has a right to compensation if he/she suffers damage by reason of any contravention of any of the requirements of the Act.
6. *Right to rectification, blocking, erasure and destruction of personal data*: The data subject on application to the Commission may cause it to order the data controller or data processor to rectify, block, erase, or destroy personal data. The procedure to be followed for erasure is set out in section 17 of the Regulations.

Cross-Border Data Sharing

Each of the provisions applies to research that uses personal data. Personal data protection law also has additional provisions that must be met when personal data is transferred outside of the country. These additional provisions are in place to ensure that data subjects continue to be protected once the data leaves the country.

Transborder (cross-border) data flow is defined as "any international cross-border flows of personal data by means of electronic transmission or other means". It *could* also include where a researcher outside of the country accesses personal data in the country. It *could* also include putting

data onto a cloud where the server is not hosted in the country. Whether it applies or not in these contexts is unsettled law.

Legal bases for transferring personal data out of Tanzania

In addition, there must be a ground under which the transfer can occur. In terms of the Personal Data Protection Act, the *legal bases* for transferring personal data out of Tanzania are:

1. *Adequacy*: A transfer of personal data to another country can occur where the country has a legal framework that provides for adequate data protection if:

   (a) the recipient establishes that the personal data is necessary for the performance of a task carried out in the public interest or for a purpose related to the lawful functions of a data controller; or

   (b) the recipient establishes the necessity of having the data transferred and there is no reason to assume that the data subject's legitimate interests may be prejudiced by the transfer or the processing in the recipient country.

   The data controller must make an initial assessment of the necessity of the transfer and the recipient of the data must verify the necessity of the transfer. The data controller must ensure that the recipient processes the personal data for the purposes for which it was transferred.

2. If a country does not have a relevant legal framework that provides for an adequate level of protection, cross-border transfer of data can also take place if an adequate level of protection is ensured in the country of the recipient and if the personal data is transferred solely to permit processing authorised to be undertaken by the data controller. An assessment of adequacy is made considering: all the circumstances of the relevant personal data transfer; the nature of the personal data; the purpose and duration of the proposed processing; the recipient country; the relevant laws in force in the third country; and the professional rules and security measures that are complied with in the recipient country.

A transfer can take place to a country that does not have an adequate level of protection on the following grounds:

1. The data subject has consented to the proposed transfer;
2. Transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of precontractual measures taken in response to the data subject's request;
3. The transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the data controller and a third party in the interest of the data subject;
4. The transfer is necessary or legally required on public interest grounds, or for the institution, trial or defence of legal claims;
5. The transfer is necessary in order to protect the legitimate interests of the data subject;
6. The transfer is made in accordance with the law, and is intended to provide information to the public, and is open for consultation either by the public or by any person who can demonstrate a legitimate interest to give his/her opinion in accordance with the conditions provided under the law; and
7. The Commission may authorise a transfer of personal data to a recipient country or any other country which does not have an adequate level of protection in its laws if the data controller satisfies the Commission that there are adequate safeguards for the protection of personal data, the fundamental rights and freedoms of the data subject and the exercise of the data subject's rights, and that such safeguards can be appropriated through adequate legal and security measures and contractual clauses.

Procedure for transferring personal data outside of Tanzania (including information required by the application)

The procedure for transferring personal data outside of Tanzania is set out in the Regulations. A data controller or data processor who intends to transfer personal data outside the country must apply for a permit using Form No. 7 which is set out in the First Schedule to these Regulations. The application must include the following information:

- particulars of the applicant, recipient and data subject;
- the type of personal data to be transferred;

- the purpose and necessity of transferring personal data;
- details of the security of personal data in the country of the recipient;
- consent of the data subject;
- date and time of sending personal data; and
- any other information required by the Commission.

In addition, at the time of application, proof must be submitted that

- the country receiving the personal data has ratified an international agreement providing requirements for the protection of personal data;
- there is an agreement between the Tanzania and the country receiving the personal data on the protection of personal data; or
- there is a contractual agreement between the person requesting the personal data and the recipient of the personal data who is outside the country.

Reasons for rejection of an application

The Commission must consider an application within 14 days, after which time it can reject or approve a permit. An application may be rejected for the following reasons:

- the transfer of personal data endangers national security;
- the Commission is satisfied that there is no adequate protection of personal data in the country of the recipient;
- the transfer of personal data is restricted by other written laws;
- application for a permit to transfer personal data does not meet the requirements of Regulation 20;
- other reasonable grounds which the Commission may deem necessary in the public interest.

The permit will be issued subject to the following conditions:

- The personal data must be transferred to the recipient authorised in the permit.
- The personal data transferred must be processed for the intended purpose only.

- The personal data must not be disclosed or transferred to another recipient without the approval of the Commission.
- The processing of personal data outside the country must not violate the laws of the country.