KENYA

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 DPA, 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 DPA and to begin to assist users in navigating the DPA. It is not comprehensive, and users of the DPA 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 Kenya, the Data Protection Act, 2021 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 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, Kenya has not yet ratified the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention).

The relevant national health legislation is the National Health Act, 2019, the Science Technology and Innovation Act, 2013, and the Digital Health Act, 2023. Furthermore, numerous policies, regulations and guidelines are relevant to health research in Kenya, including:

- Data Protection (General) Regulations, 2021
- In terms of the Data Protection Act, the Office of the Data Protection Commissioner has produced several guidance notes relevant to health research, including:
    - ODPC Guidance Note on Registration of Data Controllers and Data Processors
    - ODPC Guidance Note on Data Protection Impact Assessment
    - ODPC Guidance Note on Consent
    - ODPC Guidance Note on the Processing of Health Data, 2023
- Kenya Health Policy 2014–2030
- Science, Technology and Innovation Policy 2020–2030
- Ethical Guidelines for Public Health Emergencies in the Response to Covid-19 Pandemic in Kenya, 2020
- Guidelines for Accreditation of Institutional Ethics Review Committees in Kenya, 2017
- National Guidelines for Ethical Conduct of Biomedical Research Involving Human Participants in Kenya, 2020
- National Guidelines for Registration of Research Institutions in Kenya, 2020
- National Guidelines for Registration, Licensing, and Regulation of Researchers in Kenya, 2022

These laws, policies, regulations and guidelines set out the legal and ethical requirements that must be met for the conduct of research in Kenya and must be complied with when data is being transferred across borders.

International collaborative research requires the involvement of a Kenyan PI.

Data Protection Act, 2019

The Data Protection Act, 2019 and its Data Protection (General) Regulations, 2021 apply to the processing of all personal data, but in acknowledging the importance of research, special provisions are in place that deal with the processing of personal data for research purposes.

Personal data that is processed for research purposes only is exempt from the provisions of the Act if: it is processed in compliance with the relevant conditions; and results of the research or resulting statistics are not made available in a form which identifies the data subject. This means that the relevant provisions of the Act for research must be complied with and research results and research stats cannot be made available in a form that identifies the data subject.

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 Act are listed and discussed below. This is not a thorough assessment of the 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 Data Protection Act

	Legal definition	Layman explanation
Data subject	An identified or identifiable natural person who is the subject of personal data.	The person to whom the data relates.
Data controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.	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).
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.	Someone that 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 Commissioner	The person appointed under the Act.	The independent person established to monitor and enforce compliance with the law.
Data Protection Officer	Not defined in the Act. However, they are appointed in terms of the Act.	An individual in an organisation who is appointed to advise and to promote compliance with the law.
Identifiable natural person	A person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical,	A person who can be identified using any relevant information that belongs to him or her.

	physiological, genetic, mental, economic, cultural or social identity.	
Third party	Natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.	

Categories of Data Listed in the Data Protection Act

	Legal definition	**Layman explanation**
Personal data	Any information relating to an identified or identifiable natural person.	Data about a particular person that can identify him or her.
Sensitive personal data	Data revealing the natural person's race; health status; ethnic social origin; conscience; belief; genetic data; biometric data; property details; marital status; family details including names of the person's children, parents, spouse or spouses; sex; and sexual orientation.	Personal data 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 such that it can no longer be attributed to a specific data subject without the use of	Data where the direct identifiers have been removed (e.g., a name) so that it is impossible to identify the person without adding other information.

	additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.	This is often called coded data. Data protection law still applies to pseudonymised data.
Anonymous data	Not defined.	Data where it is no longer possible to identify a person from the data. It must be impossible to re-identify the person. Data protection law does not apply to anonymised data.
Anonymisation	The removal of personal identifiers from personal data so that the data subject is no longer identifiable.	

While data protection law does not usually apply to anonymised data, neither Kenya's Data Protection Act nor its Regulations explicitly exclude anonymised data from the ambit of their provisions. According to the Act, anonymisation means "the removal of personal identifiers from personal data so that the data subject is no longer identifiable". The Act provides that data must be anonymised in a way that ensures "the data subject is no longer identifiable". Unfortunately, the Act and the General Regulations do not contain standards for non-identifiability. While the test for anonymisation remains elusive, Kenya's 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 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 Data 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 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.
- Health and 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 by Every Data Controller or Data Processor in Terms of the Data Protection Act

The ODPC Guidance Note on the Processing of Health Data, 2023, provides further guidance on these principles and scenarios to illustrate the application of the principle in practice.

1. *Data must be processed in accordance with the right to privacy of the data subject:* Personal data should be processed such that it 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.
2. *Data must be processed lawfully, fairly and transparently in relation to any data subject:* 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 as set out in the Act. The processing of sensitive personal data is generally not permitted unless it falls within one of the grounds as set out in the Act.
3. *Data must be collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes:* Personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that the purpose must be clearly set out.
4. *Data collected must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed:* Only the data necessary for the specific purpose should be collected and processed. Only the minimum amount of data required to achieve the objectives of the data processing must be used. The data can be further processed if it is used for historical, research or statistical purposes. The data controller or data processor would have to ensure that the further processing of data is carried out solely for such purposes and will not be published in an identifiable form. Personal data processed for research purposes is exempt from the provisions of the Act if it is processed in compliance with the relevant conditions. Furthermore, if the results of the research or statistics are not available in a form that identifies the data subject, then personal data is exempt.
5. *The 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:*

Personal data must be accurate and, where necessary, kept up to date. Processes should be in place to ensure that all personal data collected is accurate.

6. *The data must be kept in a form that identifies the data subject for no longer than is necessary for the purposes for which it was collected:* Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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.
7. *Data should not be transferred outside Kenya unless there is proof of adequate data protection safeguards or consent from the data subject:* Personal data may only be transferred to another country after receipt of proof to the Data Commissioner on appropriate safeguards in respect of the security and protection of the personal data and this includes jurisdictions with commensurate data protection laws. The transfer must also be necessary for any matter of public interest. In relation to sensitive personal data, consent from the data subject and obtaining confirmation of appropriate safeguards is required, among other things.

Data Subject Rights in Terms of the Data Protection Act

The ODPC Guidance Note on the Processing of Health Data, 2023, provides further guidance on these rights and scenarios to illustrate their application in practice.

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

1. *Right to be informed about how their personal data will be used:* The data subject has the right to be informed about what his/her personal data will be used for.
2. *Right to access their personal data in the custody of the data controller or data processor:* The data subject has the right to access personal data that the data controller has about them. The data controller should have a process in place to facilitate this.
3. *Right to object to the processing of all or part of their personal data.*

4. *Right to rectification of false or misleading data:* The data subject has the right to have inaccurate personal data corrected and incomplete data completed.
5. *Right to erasure of false or misleading data about them:* The data subject has the right to request that their data be erased.
6. *Right to restriction of processing:* The data subject can request that the data controller stop processing their personal data.
7. *Right to data portability:* The data subject has the right to move their data from one data controller to another.
8. *Right to object to the processing of all or part of their personal data:* The data subject can object to the processing of their personal data where the lawful basis of processing is not consent.
9. *Right to object to automated individual decision-making:* The data subject has the right to object to a decision based solely on automated processing.

Cross-Border Sharing of Personal Data

Each of the general provisions discussed above applies to any research that uses personal data. However, the Data Protection Act, 2019, has additional provisions that must be complied with when personal data is to be 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.

While cross-border data sharing is not defined in data protection law, the laws on cross-border data sharing apply to information sent to a data controller in another country. 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 does apply in these contexts is still not settled law.

In addition, there must be a ground under which the transfer can occur.

***Legal Bases* for Transferring Personal Data out of Kenya in Terms of Data Protection Act**

1. The data controller or processor provides the Data Commissioner with evidence of appropriate safeguards with respect to the security and protection of personal data.
2. Transfer is necessary for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request.
3. Transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another person.
4. Transfer is necessary for any matter of public interest.
5. Transfer is necessary for the establishment, exercise or defence of a legal claim.
6. Transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
7. Transfer is necessary for compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

Furthermore, the ODPC Guidance Note on the Processing of Health Data, 2023, requires that the data controller must document the transfer and provide documentation to the Data Commissioner upon request.

Cross-Border Sharing of Sensitive Personal Data

The cross-border sharing of sensitive personal data out of Kenya is permissible only if the data subject has consented and there are appropriate safeguards. The transferring entity may enter into a written agreement with the recipient to spell out the provisions for accessing a robust information system and identifying countries and territories to which a transfer of personal data may be undertaken.

If sensitive personal data is shared on this ground, the Data Commissioner may request a demonstration of the effectiveness of the security safeguards or the existence of compelling

legitimate interests. Therefore, it is good practice for researchers to keep a record of these safeguards or interests.

The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfers to such conditions as may be determined.

The Cabinet Secretary may prescribe a certain nature of processing that may be effected only through a server or data centre located in Kenya based on the grounds of the strategic interests of the state or protection of revenue.