RWANDA

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 DPP Law, 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 DPP Law and to begin to assist users in navigating the DPP Law. It is not comprehensive, and users of the DPP Law 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 Rwanda, the Protection of Personal Data and Privacy 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 statute

introduced to specifically regulate research, it applies to research that involves the processing of personal data. It is only one of the several laws that must be complied with when transferring 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 came into force in June 2023. Rwanda has ratified the Malabo Convention.

The relevant national legislation is Law No. 40/2017 Establishing the National Council for Science and Technology and determining its mission, organisation and functions, and Rwanda FDA Law No. 003/2018. There are also numerous laws, regulations and guidelines, including:

- Health Sector Policy, 2015
- Health Sector Research Policy, 2012
- Law Establishing the National Cyber Security Authority and Determining its Mission, Organization and Functioning, 2017
- Ministerial Instructions No 003/2010
- Regulations governing the conduct and inspection of Clinical Trials in Rwanda
- Rules and Regulations for Research Activities (In accordance with the Ministerial Instructions No 003/2010 published in the official Gazette of the Republic of Rwanda Regulating research activities in Rwanda)

These set out the legal and ethical requirements that must be met for the conduct of research in Rwanda. There are no additional requirements that must be met in the cross-border sharing of data.

Law on Data Protection and Privacy

In addition to these legal and ethical requirements, the Law on Data Protection and Privacy applies to the processing of all personal data, and like many data protection regulations there are some

special provisions in place for research. The conditions set out in the Law all must 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 this Act are discussed below. Please note that this is not a thorough assessment of the Law on Data Protection and Privacy 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 Law on Data Protection and Privacy

	Legal definition	Layman explanation
Data subject	A natural person from whom, or in respect of whom, personal data has been requested and processed.	The person to whom the data relates.
Data controller	A natural person, public or private corporate body or legal entity which, alone or jointly with others, processes personal data and determines the means of its processing.	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	Natural person, public or private corporate body or legal entity, which is authorised to process personal data on behalf of the data controller.	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.
National Cyber Security Authority		The independent body established to monitor and enforce compliance with the law

Data Protection Officer	Not defined in the Act.	An individual in an organisation who is appointed to advise and promote compliance with the law.
Third party	Natural person, corporate body or legal entity other than the data subject, the data controller, the data processor or persons who, under the authority of the data controller, are authorised to process personal data.	

Categories of Data Listed in the Law on Data Protection and Privacy

	Legal definition	**Layman explanation**
Personal data	Information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular 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, psychological, genetic, mental, economic, cultural or social identity of that natural person.	Data about a particular person that can identify him or her.
Sensitive personal data	Information revealing a person's race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic	Personal data that is sensitive for a particular person, such as health data and genetic data, and which receives additional legal protection.

	or biometric information, sexual life, or family details.	
Pseudonymisation	The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, which is kept separately.	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. This is often called coded data. Data protection law still applies to pseudonymised data.
Anonymous data	No legal definition is provided.	Data where it is no longer possible to identify a person from it. It must be impossible to re-identify the person. Data protection law does not apply to anonymised data.

Generally, 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 Law Relating to the Protection of Personal Data and Privacy, like many other data protection laws, applies specifically to "the processing of personal data".

The Law refers to "de-identified" data and "pseudonymisation". Pseudonymisation is when information is removed from the data so that it is impossible to identify an individual, and that information is kept separate by using technical and organisational measures. Data that has been pseudonymised does fall under the Law.

Although "de-identified" data is mentioned in the Law, it is not defined. The Law provides that it is an offence to knowingly, recklessly or intentionally re-identify data that has been de-identified. It appears from this context that de-identification is a reversible technique. It is unclear whether this data is exempt from the Law. Several types of data are considered personal:

- personal data;

- sensitive personal data (including genetic or biometric data);
- pseudonymised data; and
- de-identified data

The first three kinds of data (personal, sensitive personal (including genetic) data, and pseudonymised data) are defined. An assessment would need to be made to consider whether data falls under these definitions. Unfortunately, given the lack of a definition of de-identified data, it is unclear what qualifies as de-identified data. Furthermore, whether pseudonymisation is merely a safety measure or whether it amounts to non-personal data in the hands of the data recipient who does not have access to the identifying data set is also unclear.

What is clear though is that data that is not personal data does not fall under the Law. This is often known as anonymous data. 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 whether 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.
- 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.

Special Note Regarding Genetic and Genomic Data

Genetic data is considered sensitive personal data. It has a higher level of protection under data protection law. There is ongoing debate about whether genomic datasets can ever truly be considered not to be personal data, in particular as genetic data is an identifier. In its definition of genetic and biometric data, the Law expressly provides that genetic data is sensitive personal data. Therefore, in deciding whether a genomic dataset can be considered to fall outside of the definition of personal data, context matters. It is important to consider whether the data allows anyone to identify the data subject.

Key Principles That Must be Met in Terms of the Law Relating to the Protection of Personal Data and Privacy

1. *Personal data is processed lawfully, fairly and transparently:* 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 Law.
2. *Data is 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. Therefore, the purpose must be clearly set out.

3. *Data is related to the purposes for which its processing was requested:* Only the data that is necessary for the specific purpose should be collected and processed. It is essential that only the minimal amount of data that is required to achieve the objectives of the data processing is used.
4. *Data is accurate and, where necessary, kept up to date, with every reasonable step being 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.
5. *Data is 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:* 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, one must still have a lawful basis to do so.
6. *Data is processed in compliance with the rights of data subjects:* The data controller is responsible for, and must be able to demonstrate compliance with, the principles mentioned above. It is good practice to keep a record of data processing activities, measures introduced to protect the data, and any risk assessments made. This can be used to demonstrate compliance in the event of a breach.

Data Subject Rights in Terms of the Law Relating to the Protection of Personal Data and Privacy

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

1. *Right to personal data:* The data subject has the right to request from the data controller information relating to the purposes of the processing of personal data and to access personal

data that the data controller has about them. The data controller should have a process in place to facilitate this.

2. *Right to rectification:* The data subject has the right to have inaccurate personal data corrected and incomplete data completed.
3. *Right to erasure of personal data:* The data subject has the right to request that his/her data is erased. There is an exception where processing is necessary for the public interest or for historical, statistical, or scientific research.
4. *Right to restriction of processing of personal data:* The data subject can request that the data controller stop processing his/her personal data.
5. *Right to personal data portability:* The data subject has the right to move his/her data from one data controller to another.
6. *Right to object:* The data subject can object to the processing of his/her personal data where the lawful basis of processing is not consent. This right can be deviated from if the data processor or data controller can show that there are legitimate reasons for the processing of personal data.
7. *Right to not be subject to a decision based on automated data processing:* The data subject has the right to object to a decision based solely on automated processing. This right can be deviated from if the decision was based on the explicit consent of the data subject, the decision was necessary for the contract, or the decision was authorised by law and there are safeguards in place to protect the rights of the data subject.
8. *Right to designate an heir to personal data:* The data subject has a right to designate an heir in his/her will who exercises rights when it comes to the processing of personal data.

Cross-Border Transfer of Personal Data

When considering the cross-border sharing of data for research, all the provisions of the Law Relating to the Protection of Personal Data and Privacy must be met. The Law also has a number of provisions on the cross-border sharing of data which, in addition to the other provisions, must be met.

Cross-border data sharing is not defined. It would apply when the data is being sent to a data controller/responsible party in another country. It *could* also include when a researcher outside of the country accesses the 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 or not is not yet settled law.

Lawful grounds for the cross-border flow of data

The possible lawful grounds for the cross-border flow of data are:

1. The data controller or data processor must obtain authorisation from the supervisory authority after providing proof that the outside country has appropriate provisions;
2. The data subject has provided his/her consent; or
3. If the transfer is necessary for the performance of a contract between the data subject and data controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
4. If the transfer is necessary for the performance of a contract between the data controller and third party that would benefit the data subject; or
5. If the transfer is necessary for the public interest; or
6. If the transfer is necessary for the establishment, exercise or defence of a legal claim; or
7. If the transfer is necessary to protect the interest of a data subject or of another person where the data subject is physically or legally unable to give their consent; or
8. If the transfer is for compelling legitimate interests pursued by the data controller or by the data processor and these interests do not override the interests, rights and freedoms of the data subject. This ground can apply only if the transfer is not repetitive and concerns only a limited number of data subjects, and the data controller or the data processor has assessed all the circumstances of the data transfer and has, on the basis of that assessment, provided suitable safeguards for the protection of personal data; or
9. The transfer is for the performance of international instruments ratified by Rwanda; or
10. The supervisory authority can decide to add regulation determining another reason for sharing or transferring personal data to a third party outside Rwanda.

Contract for transfer of personal data

- In addition, if a data controller or data processor authorises a person to access personal data, or share or transfer the data to a third party outside Rwanda, they must enter into a written contract with such a person. This contract must set out the respective roles and responsibilities of each party to ensure compliance with the Law.
- The supervisory authority may, by a regulation, determine the form of the contract to be used for transfer of personal data outside Rwanda.
- The supervisory authority may also require the data controller or data processor to demonstrate their compliance with the provisions of the Law and, in particular, with personal data security safeguards and interests referred to in the Law.
- In addition, the supervisory authority may prohibit or suspend the transfer of personal data outside Rwanda in order to protect the personal rights and freedoms of the data subject.

Storage of personal data outside of Rwanda

The storage of personal data outside Rwanda is permitted only if the data controller or the data processor holds a valid registration certificate authorising him or her to store personal data outside of Rwanda, and if this certificate is issued by the supervisory authority.