SOUTH AFRICA

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 (POPIA) is provided. This includes what data POPIA applies to, the categories of data, the key individuals in POPIA, 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 POPIA and to begin to assist users in navigating the Act. It is not comprehensive, and users of POPIA 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 information is governed by several laws and regulations, which must be carefully considered and complied with before researchers share data for research purposes. In South Africa, the Protection of Personal Information Act is a general data protection law that applies to the processing (i.e., use) of personal information in all sectors. While it is not a

statute introduced specifically to regulate research, it applies to research that involves the processing of personal information. It is only one of several laws that must be complied with when transferring personal information 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, South Africa has not yet ratified the African Union Convention on Cyber Security and Personal Data Protection ('the Malabo Convention').

The relevant national health legislation, regulations and guidelines are the National Health Act (NHA). Numerous regulations and guidelines have been made in terms of the NHA, including:

- Department of Health (2015): Ethics in Health Research: Principles, Processes and Structures Guidelines, 2nd edition
- Department of Health (2020): South African Good Clinical Practice: Clinical Trial Guidelines, 3rd edition
- National Health Act: Material Transfer Agreement of Human Biological Materials (SA MTA) of July 2018
- Regulations Relating to Research with Human Participants GN R719 GG 38000 September 2014
- Regulations Relating to the Import and Export of Human Tissue, Blood, Blood Products, Cultured Cells, Stem Cells, Embryos, Foetal Tissue, Zygotes and Gametes GN R181 GG 35099 of March 2012
- The South African Medical Research Council (2018): Guidelines on the Responsible Conduct of Research

These laws, regulations and guidelines set out the legal and ethical requirements that must be met for the conduct of research in South Africa and must be considered when effecting cross-border data transfer of personal information. Furthermore, if health researchers seek to transfer any human

biological material (along with its accompanying data), the National Material Transfer Agreement (SA MTA) requires that a relevant Human Research Ethics Committee (HREC) first approves the MTA before a transfer can occur.

Protection of Personal Information Act (POPIA)

In addition to these legal and ethical requirements, POPIA applies to the processing of all personal information, but in acknowledging the importance of research, special provisions are in place that deal with the processing of information purely for research purposes. In addition, extra conditions must be met prior to the transfer of personal information across borders.

Some of the techno-legal terms used in this Act are listed and 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 information for research.

The Main Actors Defined in the Protection of Personal Information Act

	Legal definition	**Layman explanation**
Data subject	The person to whom personal information relates.	
Responsible party	A public or private body or any other person who, alone or in conjunction with others, determines the purpose of and means for processing personal information.	The person who decides how the data will be used in research. Legal responsibility falls on the PI *and* on the research institution (as the employer).
Operator	A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.	The person who is not directly employed by the data controller but who is processing personal information under the direction of the data controller. This person may be a consultant, for example.
Information Regulator	The Information Regulator is established in terms of the Act.	The independent body established to monitor and enforce compliance with the Act.

Information Officer	Of, or in relation to, a: (a) public body, which means an Information Officer or Deputy Information Officer as contemplated in terms of the Act; or (b) private body, which means the head of a private body as contemplated in the Act.	An individual in an organisation who is appointed to advise and promote compliance with the Act.

Categories of Data Listed in the Protection of Personal Information Act

	Legal definition	**Layman explanation**
Personal information	Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person;	Information about a particular person that can identify him or her.

	(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.	
Special personal information	This is referred to in the Act as follows: A responsible party may, subject to section 27, not process personal information concerning: the religious or philosophical beliefs, race or ethnic origin, trade union membership, political	Sensitive personal information about a particular person, such as health data and genetic data, and which receives additional legal protection.

	persuasion, health or sex life or biometric information of a data subject.	
De-identify	In relation to personal information of a data subject, this means to delete any information that: (a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.	To de-identify personal information, any information that can be used to identify a data subject is deleted, and therefore only non-personal information remains. It is an important requirement that no one else, using a method which the data controller could have reasonably foreseen, should be able to re-identify the data subject.

Information is considered personal when it relates to an identified or identifiable person. It is this personal information that data protection law seeks to protect. Data protection law does not concern or apply to de-identified non-personal information. De-identified data is explicitly excluded from POPIA. This is particularly useful for scientists who, by de-identifying their information, will not need to comply with data protection laws. De-identifying information is the process of stripping the data of any information which can be used to identify a data subject. It should not be possible to re-identify the data subject, directly or indirectly, by manipulating the information or linking it with other information. It can be challenging to assess whether the information intended to be shared is de-identified, especially in the light of fast-paced technological advancements powered by artificial intelligence. While there is no guidance from the Regulator on this point, general principles are worth highlighting.

The GDPR, for instance, adopts a risk-based approach, considering factors such as the likelihood of re-identification, and considering cost, time, and technological advancements. POPIA, on the other hand, focuses on whether a *reasonably foreseeable* method exists that could re-identify a

data subject. Unlike the GDPR, POPIA's test does not require that the method is *likely* to be *used*; it is enough that the method foreseeably *exists*.

Another measure worth considering is pseudonymisation. Although not mentioned in POPIA, the South African proposed Code of Conduct for Research recognises pseudonymisation as an important security measure. There is still uncertainty about whether pseudonymised data can be deemed de-identified information if it is in the hands of a data recipient who lacks the means to identify a data subject. The exact nature of pseudonymised datasets in this context requires further clarification in the South African legal landscape.

On this, there are two possibilities:

1. Is there anyone in the world who can identify the data subject from the data? (This is an objective test that determines whether anyone would be able to identify the data subject.)
2. Can a specific holder of the data identify the data subject from the data? (This is a context-specific test from the perspective of the data recipient, and whether he or she would be able to identify the data subject.)

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 data Controller B, the dataset would not be de-identified non-personal information.

The second context-specific 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 Data Controller B, the dataset *may* be considered de-identified non-personal information in the hands of Data Controller B. A test would be needed to determine whether the dataset is de-identified in the hands of Data Controller B.

In the absence of direction from the Regulator on a test, it will be for the responsible party to decide. In making this decision, general points may be worth bearing in mind (many of which derive from guidance related to anonymisation under the GDPR):

- An assessment must be made on a case-by-case basis, considering the particular context.
- The de-identification must be irreversible.
- The assessment is made on the current state of the art. As technology progresses, information once deemed to be de-identified may become personal information 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, such as whether a method of re-identification is *reasonably likely* to be used (considering, for example, technology, resources and time to identify the data subject) so that it is possible to take appropriate steps to guard against these risks. However, this is insufficient to comply with POPIA's test for de-identification. If a reasonably foreseeable method *exists* that can be used to identify the data subject, no matter how unlikely that it could be used, the information will remain personal information.
- It is possible to follow the GDPR test which states the data is anonymous if an individual cannot be singled out, or identifiers cannot be linked to make a person identifiable, or if it is impossible to infer a link between two pieces of information in a dataset.
- Genetic data is considered to be special personal information. It not only falls under the data protection law but also has a higher level of protection under POPIA.
- There is an ongoing debate about whether genomic datasets can ever be rendered truly de-identified, in particular as genetic data is an identifier. In considering whether a genomic dataset can be considered de-identified, context matters – i.e., consider the objective factors related to the information.

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

1. *Purpose specification*: Personal information 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. There are certain exceptions for research.

2. *Processing limitation*: Only the data that is necessary for the specific purpose should be collected and processed.
3. *Information quality*: Personal information must be accurate and, where necessary, kept up to date. Processes should be in place to ensure that all personal information collected is accurate.
4. *Further processing limitation*: The processing of personal information should be used only for the purpose for which it was collected, unless the purpose falls within one of the exceptions (for example, research).
5. *Openness*: The responsible party must maintain documentation of all processing activities and inform the data subject about the processing of his/her personal information.
6. *Data subject participation*: This details the rights of the data subject. There are some exceptions for research.
7. *Security safeguards*: Personal information 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.
8. *Accountability*: The responsible party 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 Under the Protection of Personal Information Act

Data subjects have rights that the responsible party must protect. These rights are the:

1. *Right to be informed*: The data subject has the right to be informed about what their personal information will be used for. This right can be exempted if the personal information has not been collected directly from the data subject and the processing is for research.
2. *Right to access*: The data subject has the right to access personal information that the responsible party has about them. The responsible party should have a process in place to facilitate this.

3. *Right to rectification*: The data subject has the right to have inaccurate personal information corrected and incomplete data completed.
4. *Right to erasure*: The data subject has the right to request that his/her data be erased.
5. *Right to restriction of processing*: The data subject can request that the responsible party stop processing his/her personal information.
6. *Right to object*: The data subject can object to the processing of his/her personal information where the lawful basis of processing is not consent.
7. *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 information which is intended to provide a profile of the data subject.

Some rights can be exempted from in the context of research.

Cross-Border Data Sharing

Each of the provisions applies to any research that uses personal information. Data protection law also has additional provisions that must be met when personal information is to be transferred outside of the country. These additional provisions are in place to ensure that data subjects continue to be protected once their data leaves the country. While cross-border data sharing is not defined in POPIA, the laws on cross-border data sharing clearly apply to information sent to a responsible party in another country. It *could* also include where a researcher outside of the country accesses personal information 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 does not apply in these contexts is still not settled law. In addition, there must be a ground under which the transfer can occur.

In terms of POPIA, the *legal bases* for transferring personal (including health) information outside of South Africa are:

1. There must be an adequate level of protection in the form of a law, binding corporate rules (BCR) or a binding agreement (data transfer agreement (DTA)).
2. The data subject consents to the transfer.

3. The transfer is necessary for facilitating a contract between the data subject and the responsible party.
4. The transfer is necessary for a contract, in the interest of a data subject, between the responsible party and a third party.
5. The transfer is for the benefit of the data subject and not the general public.