BOTSWANA

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 data is governed by several legal and ethical regulations, all of which must be met prior to the sharing of data for research. The Data Protection Act delineates the rights and duties of parties that process personal data and establishes the Information and Data Protection Commission, which is responsible for ensuring that the Data Protection Act is properly applied. The Data Protection Act is a general data protection law that applies to the processing (i.e., use) of

personal data in all sectors and was not introduced to regulate research. However, as research processes vast quantities of personal data, the Data Protection Act applies. The Data Protection Act is only one of several laws that must be complied with when transferring data for research.

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). However, Botswana has not ratified the Malabo Convention.

The relevant national laws on health research in Botswana are:

- Constitution of the Republic of Botswana
- Public Health Act
- Data Protection Act
- National Health Policy, 2011
- National Policy on Research, Science, Technology, and Innovation, 2012
- The Ministry of Environment, Natural Resources Conservation and Tourism Research Guidelines, 2019, which mention genetic resources (but not health research)

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

Data Protection Act

In addition to these legal and ethical requirements, the Data Protection Act applies to the processing of all personal data and this includes research. Because of the importance of research, there are special provisions in place for it. Provision is also made for health data and genetic data. Sensitive personal data may be processed for health or medical purposes where it is necessary for preventive medicine and the protection of public health, medical diagnosis, healthcare, or the management of health and hospital care services. The Data Protection Act also provides that the

processing of genetic data and biometric data, if processed for what it reveals or contains, is prohibited, except where the processing is in accordance with the Data Protection Act's provision on the processing of sensitive personal data. Where genetic and biometric data are processed for medicinal purposes and consent has been obtained from the data subject, such data will be processed only if a unique patient identification number is provided. In addition, extra conditions must be met prior to the transfer of personal data across borders.

Some of the techno-legal terms used in the Data Protection Act are discussed below. This is not a thorough assessment of the 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 individual who is the subject of personal data.	The person to whom the data relates.
Data controller	A person who alone or jointly with others determines the purposes and means for which personal data is to be processed, regardless of whether such data is processed by such a person or agent on that person's behalf.	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 person who processes data on behalf of the data controller.	Someone that is not directly employed by the data controller, but who is processing personal data under the direction of the data controller. They may be a consultant, for example.

Data protection representative	A person who is appointed by the data controller, who must independently ensure that personal data is processed correctly and lawfully.	
Commission	The Information and Data Protection Commission.	The independent body established to monitor and enforce compliance with the law
Commissioner	Commissioner of the Information and Data Protection Commission.	An individual in an organisation who is appointed to advise and promote compliance with the law.
Third party	A person other than the data subject, data controller, data processor, data protection representative and such other person authorised by the data controller or data processor.	
Tribunal	The Information and Data Protection Appeals Tribunal.	
Recipient	A person to whom personal data is provided, but does not include (a) a person who received data in the framework of a particular legal proceeding; and (b) the Commissioner, when the personal data is provided in order to perform the duty to supervise, control or audit.	

Categories of Data Listed in the Data Protection Act

	Legal definition	Layman explanation
Personal data	Information relating to an identified or identifiable individual, which individual can be identified directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to the individual's physical, physiological, mental, economic, cultural or social identity; and 'data' must be construed accordingly.	Data about a particular person that can identify him or her.
Sensitive personal data	Personal data relating to a data subject which reveals his or her (a) racial or ethnic origin; (b) political opinions; (c) religious or philosophical beliefs; (d) membership of a trade union; (e) physical or mental health or condition; (f) sexual life; (g) filiation; or (h) personal financial information, and includes (a) any commission or alleged commission by him or her of any offence; (b) any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings, or the sentence of any court in such	Personal data about a particular person which is considered sensitive, such as health data and genetic data, and which receives additional legal protection.

	proceedings; and (c) genetic data, biometric data and the personal data of minors.	
Biometric data	Any information stemming from the statistical analysis of biological data.	
Genetic data	Personal data relating to the inherited or acquired characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.	

Data protection law does not apply to anonymised data. While anonymised data is not specifically excluded from the application of the Data Protection Act, it clearly applies only to personal data, and so data that is rendered no longer personally identifiable will presumably fall outside the ambit of the Data Protection Act.

To determine whether data is anonymised, it is important to make an assessment. This can be difficult. There is no guidance from the Commission 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.

Without direction from the Commission on a test, it will be for the data controller 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 laws.
- 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.
- It is possible to follow the GDPR test which states if an individual cannot be singled out, or identifiers cannot be linked to make a person identifiable, or that it is impossible to infer a link between two pieces of information in a dataset, and then the data is anonymous.
- Genetic data is considered to be sensitive personal data. It not only falls under the data protection laws, 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 – i.e., the objective factors associated with the data.

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

1. *Lawfulness and fairness*: Personal data must be processed fairly, lawfully, and with the knowledge or consent of the data subject, where appropriate. The processing of sensitive personal data is generally not permitted unless it falls within one of the grounds as set out in the Data Protection Act. There is a special provision for the processing of personal data for research purposes in terms of the Data Protection Act. However, the use of genetic data is restricted further and it can only be processed under the grounds in the Data Protection Act. For genetic data and its use in research, consent is probably the only lawful basis for the processing of personal data.
2. *Adequacy*: Personal data must be adequate and relevant in relation to the purpose for processing.
3. *Accuracy and completeness*: Personal data must be accurate, complete, and kept up to date.

4. *Purpose limitation*: Personal data should be collected for specific, explicit, and legitimate purposes and not processed in a manner that is incompatible with those purposes. This means that the purpose must be clearly set out. The Data Protection Act has a special provision for the processing of personal data for scientific purposes.
5. *Security*: Personal data must be protected by reasonable security safeguards against risks such as loss, unauthorised access, destruction, use, modification, or disclosure. The data controller must ensure that where personal data is processed for scientific purposes and is kept for longer than necessary, appropriate security safeguards are in place.
6. *Completeness and correction*: Where data is incomplete or incorrect, reasonable measures should be taken to complete, correct, block, or delete the personal data, taking into account the purpose of the processing.
7. *Storage limitation*: Personal data should not be kept for longer than is necessary for the purposes for which the personal data is processed. 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.
8. *Good practice*: Personal data should be processed in line with good practice.
9. *Processing limitation*: Personal data will not be used, made available, or disclosed for any other purpose than that which has been specified, unless the data subject has consented or it is authorised by law.

Data Subject Rights Under the Data Protection Act

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

1. *Right to information*: When personal data is collected directly from the data subject, the data controller or data processor must provide the data subject with certain information, including: the identity and address of the data controller or data processor; the purpose of the processing of the personal data; where personal data is obtained for purposes of direct marketing, the right to object to the processing; and any additional information to ensure fair processing. Under the Data Protection Act, this applies when personal data is not collected directly from the data subject but from other sources, but this does not apply if the processing

is for scientific research. The Data Protection Act further states that the data subject has the right to obtain from a data controller or data processor confirmation of whether the data controller or data processor has personal data relating to him or her. This right can be exempted from if the use of the personal data is for scientific research.

2. *Right to access*: The data subject has a right to receive communication relating to him or her within a reasonable time, from the time of request and at a reasonable charge, if any. This right can be exempted from if the use of the personal data is for scientific research.
3. *Right to reason*: The data subject has the right to be given a reason for refusal of a request to obtain from a data controller confirmation or receive communication of personal data relating to him or her.
4. *Right to challenge*: The data subject has the right to challenge the refusal of a request to receive communication and confirmation of personal data relating to him or her, and has the right to challenge personal data and submit a complaint which, if successful, will result in the personal data being deleted, rectified, completed, or amended.
5. *Right to access, rectification, and deletion*: As part of the information provided to the data subject by the data controller or the data processor, depending on the circumstances and additional information, the data subject has the right to access, rectify and, where applicable, delete personal data concerning him or her.
6. *Revocation of consent*: Where the processing of personal data occurs with the consent of the data subject, the data subject may revoke his/her consent at any time in writing for legitimate grounds.

Cross-Border Data Sharing

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

The Data Protection Act defines ‘transborder flow’ as the international flow of personal data that can be transmitted by electronic or other forms of transmission, including by satellite. The

transborder or cross-border flow of personal data is generally prohibited unless it falls into one of the permitted grounds.

The Data Protection Act prohibits the transfer of personal data from Botswana to another country unless a country is listed in the Gazette by the Minister publishing it in an Order. The cross-border flow of personal data can take place to any country listed without need for further safeguards. The 45 countries listed in the Order are: Transfer of Personal Data Order 2022.pdf

For countries not on the list, the cross-border flow of personal data can take place only if the third country to which the data is transferred provides an adequate level of protection. The Commissioner makes an assessment that the third country to which the data is going to has an adequate level of protection. This assessment depends on the circumstances of each case, with particular consideration being given to the:

- Nature of the data
- Purpose and duration of the proposed processing operation (i.e., the research)
- Country of origin and country of final destination
- Rule of law, both general and sectoral, in force in the third country
- Professional rules and security safeguards that are complied with in that country.

If a country does not have adequate security standards and is not on the list, a transfer is generally prohibited, unless:

1. The data subject consents to the proposed transfer.
2. The transfer is necessary for the performance of a contract between the data subject and the data controller in terms of the implementation of pre-contractual measures taken in response to the data subject's request.
3. The transfer is necessary for the performance or conclusion of a contract which is concluded or to be concluded in the interests of the data subject between the data controller and a third party.

4. The transfer is necessary or legally required for the public interest, or for the establishment, exercise or defence of a legal claim.
5. The transfer is necessary in order to protect the vital interests of the data subject.
6. The transfer is made from a register that, according to any law, is intended to provide information to the public and which is open for public inspection.
7. When the Commissioner authorises a transfer of personal data to a third country that does not ensure an adequate level of security safeguards, the data controller gives adequate safeguards through appropriate contractual provisions, with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise.