ZIMBABWE

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 Act. 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 is a general data protection law that applies to the processing (i.e., use) of personal information in all sectors. Therefore, it is not a regulation that was introduced to regulate research. However, as research

processes vast quantities of personal information, the Data Protection Act applies. It is only one of several laws that must be met 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, Zimbabwe has not ratified the Malabo Convention.

The relevant national legislation is:

- Access to Information and Protection of Privacy Act
- Constitution of Zimbabwe
- Cyber and Data Protection Act
- Health Service Amendment Act
- Research Act
- Research (Constitution of the National Public Health Institute) Regulations, 2020
- National Policy for Information and Communications Technology (ICT), 2016. This was published prior to the enactment of the Data Protection Act, but one of its goals was to create a legal framework that addresses issues related to inter alia data protection. The Policy also mentions the creation of a National Data Centre, which "which allows Zimbabwe to centralize her information storage, management and protection, as well as take advantage of cloud computing opportunities".
- National ICT Policy 2022–2027

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

Data Protection Act

In addition to these legal and ethical requirements, the Data Protection Act applies to the processing of all personal information. In acknowledging the importance of research, special provisions are in place for research. Importantly for health research, the processing of genetic data, biometric data and health data is prohibited unless the data subject has given consent in writing to the processing.

The conditions set out in the Data Protection Act must all be met for research. In addition, extra conditions must be met prior to the transfer of personal information 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 information for research.

The Main Actors Defined in the Data Protection Act

	Legal definition	Layman explanation
Data subject	An individual who is an identifiable person and the subject of data.	The person to whom the data relates.
Data controller	Any natural person or legal person who is licensable by the Authority; this includes public bodies and any other person who determines the purpose and means of processing data.	The person who decides what the data will be used for in research. Legal responsibility falls on the Principal Investigator (PI) *and* on the research institution (as employer).
Data processor	A natural person or legal person who processes data for and on behalf of the data controller and under the data controller's instruction, except for	Someone that is not directly employed by the data controller, but who is processing personal information under the direction of

	the persons who, under the direct employment or similar authority of the data controller, are authorised to process the data.	the data controller. They may be a consultant, for example.
Data Protection Authority or Authority	Postal and Telecommunications Regulatory Authority of Zimbabwe, established in terms of the Postal and Telecommunications Act.	The independent body established to monitor and enforce compliance with the law.
Data Protection Officer or DPO	Any individual appointed by the data controller and who is charged with ensuring, independently, 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.
Data controller's representative or Controller's representative	Any natural person or legal person who performs the functions of the data controller in compliance with obligations set out in the Act.	
Child	Any person under the age of 18 years.	
Third party	Any natural or legal person or organisation other than the data subject, the data controller, the data processor and anyone who, under the direct authority of the data controller or data processor, is authorised to process the data.	
Identifiable person	A person who can be identified directly or indirectly, in particular by	

	reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.	
Minister	The Minister responsible for information and communications technologies.	
Health professional	Any individual determined as such in terms of the Health Professions Act.	
Recipient	A natural or legal person, agency or any other body to whom personal information is disclosed by a data controller, whether a third party or not. However, persons who receive personal information in the framework of a particular legal inquiry must not be regarded as recipients.	

Categories of Data Listed in the Data Protection Act

	Legal definition	**Layman explanation**
Personal information	Information relating to a data subject, including (a) the person's name, address or telephone number; (b) the person's race, national or ethnic origin, colour, religious or political beliefs or associations; (c) the person's age, sex, sexual orientation,	Information about a particular person that can identify him or her.

	marital status or family status; (d) an identifying number, symbol or other particulars assigned to that person; (e) fingerprints, blood type or inheritable characteristics; (f) information about a person's healthcare history, including a physical or mental disability; (g) information about educational, financial, criminal or employment history; (h) opinions expressed about an identifiable person; (i) the individual's personal views or opinions, except if they are about someone else; and (j) personal correspondence pertaining to home and family life.	
Sensitive data	Information or any opinion about an individual which reveals or contains the following: (a) racial or ethnic origin; (b) political opinions; (c) membership of a political association; (d) religious beliefs or affiliations; (e) philosophical beliefs; (f) membership of a professional or trade association; (g) membership of a trade union; (h) information on sex life; (i) criminal educational, financial or employment history; (j) gender, age, marital status or family status; (k) health information about an individual; (l)	Data about a particular person which is considered sensitive, such as health data and genetic data, and which receives additional legal protection.

	genetic information about an individual; or (m) any information which may be considered as presenting a major risk to the rights of the data subject.	
Data	Any representation of facts, concepts and information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device/system, database, electronic communications network or related devices and including a computer program and traffic data.	
Genetic data	Any personal information stemming from a DNA analysis.	

Generally, data protection law applies only to personal data. The Data Protection Act, however, applies to the processing of all data as defined in it. Despite this, many of the restrictive provisions concerning the processing and transfer of data relate specifically to personal information (and not to data generally). Therefore, if data is not considered to be personal data, a researcher may be exempt from the more restrictive processing requirements.

Different sections of the Data Protection Act refer to "personal information" and "data". This does not imply that the terms can be used interchangeably as "personal information" is best described as information that can be used to identify a data subject, clearly indicating that it is specific to the data subject and his/her unique features (e.g., racial origin, gender, genetic information). In contrast, "data" has a broader meaning as it simply includes whatever representation of facts or

information can be conveyed on a digital platform, such as a computer system, computer device or a database.

Researchers must, however, still be careful when considering the transfer of data outside of Zimbabwe. The Data Protection Act sets out the requirements for the transfer of *personal information* outside of Zimbabwe and the requirements for the transfer of *data* outside of Zimbabwe. Before considering the requirements, a researcher must know when the Data Protection Act applies.

Many other data protection regulations state that anonymised or de-identified information that cannot be re-identified is not considered to be personal data and therefore does not fall under the Data Protection Act concerned. Zimbabwe, however, does not do that. Pseudonymisation is also not specifically mentioned. The Data Protection Act does provide that "data concerning health shall be processed only if a unique patient identifier is given to the patient which is distinct from any other identification number, issued by the public authority established for this purpose". This is often what is defined as pseudonymisation and is a technique that is a requirement for the lawful processing of health data. The linking of the patient identifier to another identifier that allows the data subject to be identified is permissible only with the Authority's express permission. This, however, does not appear to exempt the data from the application of the Data Protection Act. More clarity from the Authority is needed about whether the pseudonymised dataset would be considered personal information in the hands of a recipient who does not possess the means to re-identify the data subject.

Researchers will need to make an assessment about whether the data they are holding is personal data or anonymised (i.e., not personal 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 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 Terms of the Data Protection Act

1. *Data quality*: The data controller must ensure that personal information is adequate, relevant and not excessive considering its purpose, that it is accurate and kept up to date (where necessary), and that it is kept in a form that allows for the identification of data subjects for no longer than is necessary.

2. *Accessibility*: The data controller must take appropriate steps to ensure that personal information is accessible regardless of the technology used and ensure that the evolution of technology is not an obstacle to accessing or processing such data.
3. *Lawfulness and fairness*: Personal information must be processed lawfully, fairly, transparently, and the processing must be necessary. Lawful means that there must be a legal basis for the processing of the personal information. The processing of sensitive data or genetic data, biometric data, and health data is generally not permitted unless it falls within one of the grounds in the Data Protection Act. There is a special provision for the processing of sensitive data or genetic data, biometric data, and health data for scientific research.
4. *Consent and lawful basis*: Non-sensitive personal information may be processed only if the data subject has consented to the processing, unless it is necessary in: (a) proving an offence; (b) complying with an obligation to which the data controller is subject by virtue of a law; (c) protecting the vital interests of the data subject; (d) performing a task carried out in the public interest, or in the exercise of the official authority vested in the data controller, or in a third party to whom the data is disclosed; or (e) promoting the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.
5. *Privacy*: Personal information must be processed in accordance with the right to privacy of the data subject. Furthermore, personal information should be collected only where a valid explanation is provided whenever information relating to family or private affairs is required.
6. *Purpose limitation*: 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. The further processing of data for scientific research purposes is not considered incompatible.
7. *Data minimisation*: Only the personal information that is necessary for the specific purpose should be collected and processed. The personal information must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
8. *Accuracy*: Personal information must be accurate and, where necessary, kept up to date.
9. *Storage limitation*: Personal information 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

information 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.

10. *Disclosure*: When collecting personal information from the data subject (directly or indirectly), the data controller must provide the data subject with certain information, including the details of the data controller, the purpose of the processing, the existence of the right to object, whether compliance with the request for information is compulsory, and any other supporting information. When personal information is not directly obtained from the data subject and is for research purposes, there is no need to comply with the disclosure requirement.
11. *Security*: To protect the security, integrity and confidentiality of the personal information, the data controller must protect the personal information from unauthorised or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical or organisational measures. Both organisational and technical measures must be put in place to secure the data.
12. *Accountability*: 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 Under the Data Protection Act

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

1. *Right to privacy*: The data controller must process personal information in accordance with the data subject's right to privacy.
2. *Right to be informed*: The data subject has the right to be informed about what his/her personal information will be used for. This provision can be exempted from if the personal information has not been collected directly from the data subject and the processing is for scientific research purposes and it would be impossible or would involve a disproportionate effort to inform the data subjects.

3. *Right to access*: The data subject has the right to access personal information that the data controller or data processor has about them.
4. *Right to object*: The data subject has the right to object to the processing of all or part of his/her personal information, where the lawful basis of processing is not consent.
5. *Right to correction*: The data subject has the right to have false or misleading personal information corrected. The data controller has a duty to erase or rectify any inaccurate personal information.
6. *Right to deletion*: The data subject has the right to have false or misleading personal information about him/her deleted.
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, including profiling.

Cross-Border Data Sharing

When considering the transborder/cross-border flow of personal information 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 information that, in addition to the other provisions, must be met.

The Data Protection Act defines "transborder flow" as "international flows of data by the means of transmission including data transmission electronically or by satellite".

A data controller is prohibited from transferring personal information about a data subject to a third party in another country. However, there are grounds under which the transfer of *personal information* (but not data) outside Zimbabwe can take place. They are:

Adequacy: A country or international organisation has an adequate level of protection and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out. The adequacy of the level of protection afforded by the country will be assessed in the light of all the circumstances of a data transfer operation. Particular consideration is given to the nature of the data, the purpose and duration of the proposed processing operation, the recipient country, the laws relating to data protection in force in

the country, and the professional rules and security measures that are complied with in that country.

The Authority can lay down the categories of processing operations for which and the circumstances under which the transfer of data to countries outside Zimbabwe is not authorised. It is important to check that research does not fall into one of the prohibited grounds.

The Minister responsible for the Cyber Security and Monitoring Centre may give directions on how to implement these provisions in terms of the transfer of personal information outside of Zimbabwe. Until now, no directions have been provided by the Minister.

For countries without an adequate level of protection, the transfer of personal information and data outside Zimbabwe can take place only if:

1. The data subject has unambiguously consented to the proposed transfer.
2. The 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 important public interest grounds, or for the establishment, exercise or defence of legal claims.
5. The transfer is necessary in order to protect the vital interests of the data subject.
6. The transfer is made from a register which, according to Acts or Regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the case at hand.