BOTSWANA

ACRONYMS

4IR	Fourth Industrial Revolution
AI	Artificial intelligence
DPA	Data Protection Act
GDPR	General Data Protection Regulation (Europe)
GIS	Geographical information system
HBM	Human biological material
ICT	Information and communication technology
IT	Information technology
NDP	National Development Plan
PI	Principal investigator
RSTI	Research, Science, Technology and Innovation
SDI	Spatial data infrastructure
SISE	Science and Innovation School of Excellence

MODES OF INFORMED CONSENT

This section provides legal clarity on the modes of informed consent. When data such as genomic data and personal health data are used in health research, clarity is needed on the modes of informed consent (e.g., broad, tiered or open consent) that are legally required from research participants in relation to data collection, analysis, storage, combination, sharing within a jurisdiction, and cross-border sharing.

The main data protection legislation is the Data Protection Act (2018). The standard in the Act is *specific informed consent.*

The Data Protection Act

Definition of genetic data

The Act defines genetic data as personal data relating to the inherited or acquired characteristics of a natural person which gives unique information about the physiology or health of that person and which results, in particular, from an analysis of a biological sample from the natural person in question. Most notably, genetic data contains 'unique information' about a person's physiology or health. Genetic data is also classified as sensitive personal data under the Act.

Circumstances when consent is required

In certain cases, scientists must ensure that personal data is obtained with the knowledge or consent of the data subject. Consent of the data subject may also be required when disclosing, making available or using personal data for other new purposes. Furthermore, consent may be required when processing personal data where no other criteria for processing are applicable.

Circumstances for processing sensitive personal data without consent

Processing of sensitive personal data requires consent in writing. However, sensitive personal data may be processed where (i) consent cannot be given by or on behalf of the data subject, (ii) the data controller cannot be reasonably expected to obtain the consent of the data subject, or (iii) where consent by or on behalf of the data subject has been unreasonably withheld.

Revoking consent and circumstances for legally waiving consent

The data subject may revoke his or her consent at any time, in writing, for legitimate reasons. The requirement to obtain consent may be legally waived when processing data for historical, statistical or scientific purposes.

Consent and the transfer of data to a third country

The transfer of personal data to a third country that does not ensure adequate security safeguards is prohibited. However, the consent of the data subject to the transfer waives this requirement.

INDIVIDUAL AND COMMUNITY RIGHTS IN GENOMIC DATA

This section provides legal clarity on the nature and content of individual and community rights. Legal clarity is needed on the respective rights of individual research participants and their communities (where appropriate) in genomic data, in particular. These rights potentially include benefit sharing, ownership, and co-ownership in intellectual property rights in discoveries.

Many rights relevant to human genomics research are protected under the law. These rights include the right to privacy, freedom of conscience, freedom of expression, freedom of assembly and association, freedom of scientific research, and certain rights to engage in culture. These rights are generally provided for in the Constitution and are outlined in legislation, regulations and guidelines.

Regulatory and Supporting Institutions

The institutions involved in regulating and supporting compliance with human genomic research include the:

- Botswana Innovation Hub
- Botswana Institute for Technology Research and Innovation
- Botswana Medicines Regulatory Authority
- Ministry of Health and Wellness
- National Health Research Council.

Individual and Community Benefit Sharing

Although the law is not clear on the modalities of benefit sharing, the general approach is that the maximum benefit to the nation must be prioritised. Therefore, the foreseeable risks and inconveniences are to be measured against the anticipated benefit for the individual and to society.

Benefits

(1) Tissue donation, removal and associated payment issues

With respect to tissue, organ, blood or gamete donation, any person can donate a human body or specific tissue to a person or institution. Donation is made through a will or consent to a post-mortem examination. The removal of body organs or tissues from a living person is done with the written authority of the medical practitioner responsible for clinical services in the institution concerned.

The sale and purchase of human organs, tissues, blood or gametes is prohibited and a donor cannot receive any payment or reward for such donations – except compensation for costs incurred in the process of making a donation. This is because matters concerning compensation go beyond HBM to associated data and therefore a person is not entitled to remuneration in relation to a donation of their human biological data. The purpose of organ, tissue or blood donation is limited to:

- Medical and dental training
- Medical research
- Therapeutic purposes.

(2) Patenting

Although patenting is allowed, several inventions are excluded from patenting. These include: methods for treatment of the human or animal body by surgery or therapy and diagnostic methods; and inventions meant for commercial exploitation that are necessary for the protection of public order or morality, including protection of human or animal health, plant life or to avoid prejudice to the environment.

The law is silent on patents relating to human genetic material.

GEOSPATIAL DATA FOR PUBLIC HEALTH SURVEILLANCE

This section provides legal clarity on the use of persons' geospatial data for public health surveillance. Web Geographic Information Systems are increasingly being used in public health surveillance involving infectious diseases. Privacy risks associated with the use of novel geospatial technologies (and the data generated by such technologies) are analysed and legal clarity is provided on how to comply with the law.

The use of technologies that collect geospatial data has been limited to agriculture, land ownership and management, and electricity provision. Tracking and tracing technologies have been applied to the healthcare setting to a very limited extent. However, considering the infectious health burdens such as TB and HIV/AIDS, the value of geospatial data for the monitoring, management and control of these conditions and patients is becoming clearer. However, the general understanding of these technologies is still poor and if they are to empower public healthcare, national government must create proactive strategies and implement regulations that could facilitate their use.

The current legal and regulatory framework is considered and discussed below, as are spatial data infrastructures.

Geospatial Legal Framework

There are no laws, guidelines or policies in Botswana that provide for the regulation of geospatial data. Instead, laws pertaining to data protection in general must be relied upon.

Data Protection Act

The Data Protection Act (DPA) is in force. Botswana provides for the protection of privacy in terms of the common law which includes the duty of confidentiality in most professions. If information is given in circumstances where it is expected that a duty of confidence applies, that information can normally be disclosed only with the information provider's consent. This means, for example, that all patient information can be disclosed only with the consent of the patient.

The definitions of *data controller* and *data processor* are broad. Data controller means a person who alone, or jointly with others, determines the purposes and means by which personal data is to be processed, regardless of whether such data is processed by such person or agent on that person's behalf. Data processor means a person who processes data on behalf of the data controller.

Application of data rights

Data rights	Applicable	Particulars
Right to access	Yes	
Right to withdraw	Yes	After consent, the data subject can revoke consent at any time for legitimate grounds.
Right to erasure	Yes	
Purpose of use	Specific	Personal data must not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or as may be authorised by any law.
Processing consent	Yes	
Right to object	Yes	If successful, the data subject can have personal data deleted, rectified, completed or amended.
Sensitive data	Yes	Processing of personal and sensitive personal data can be done only with the written consent of the data subject and should be obtained from the person whose data is being collected, stored and/or processed.

Personal data may be processed without the consent of the data subject where:

- processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps, at the request of the data subject, prior to entering into a contract;
- processing is necessary for complying with a legal obligation to which the data controller is subject;
- processing is necessary for performing an activity carried out in the public interest, or in exercising an official authorisation vested in the data controller or a third party to whom the data is disclosed; or
- processing is necessary for a purpose that concerns a legitimate interest of the data controller, or of a third party to whom personal data is provided, except where the interest

is overridden by the need to protect the fundamental rights and freedoms of the data subject – in particular the right to privacy.

Minimum standards of data protection provided for in the DPA:

Minimum standards	Requirements for processing by the data controller
Data is to be collected fairly and lawfully	(1) personal data is processed fairly and lawfully and, where appropriate, obtained with the knowledge or consent of the data subject; (2) personal data is processed in accordance with good practice.
Data is to be used only for the purpose for which it was collected	(1) personal data is collected for specific and legitimate purposes; (2) personal data is not processed for any purpose that is incompatible with the specified and legitimate purposes. Personal data will not be disclosed, made available or used for purposes other than those specified, except: (1) with the consent of the data subject; or (2) as may be authorised by law.
Data is to be adequate and relevant	(1) personal data that is collected is adequate and relevant in relation to the purposes of its processing.
Data is to be accurate and current	(1) personal data must be accurate, complete and current; (2) where data is incomplete or incorrect, all reasonable measures must be taken to remedy this, having regard to the purposes for which it is processed.
Data is to be kept secure	(1) personal data is protected against risks such as loss, unauthorised access, destruction, use, modification or disclosure.

	A data controller will, where sensitive personal data is processed, ensure that appropriate safeguards are adopted.
Data must be destroyed after its purpose is completed	(1) personal data is not kept for a period longer than is necessary.

Definitions

The DPA distinguishes between personal data and sensitive personal data, and also defines biometric data and genetic data:

Personal data	Information relating to an identified or identifiable individual, in particular by reference to an identification number or to one or more factors specific to the individual's identity.
Sensitive personal data	data revealing the race, health status, ethnic origin, conscience, belief, genetic information, biometric information, property details, marital status, family details, sex or sexual orientation of the data subject.
Health data	Data related to the state of physical or mental health of the data subject and includes data collected in the course of registration for or provision of health services, or data which associates the data subject with the provision of specific health services.
Biometric data	Personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation, including blood typing, fingerprinting,

DNA analysis, earlobe geometry, retinal scanning, and voice recognition.

Processing of sensitive personal data is prohibited, except where

- the processing is provided for under the Act;
- the data subject has given consent;
- the data subject has made the data public;
- the processing is
    - necessary for national security;
    - necessary for exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment; or
    - authorised by any other law, because of substantial interest of the public; or
- the processing is necessary to protect the vital interests of a data subject or another person where
    - consent cannot be given by or on behalf of the data subject;
    - the data controller cannot be expected to obtain consent of the data subject; or
    - consent by or on behalf of the data subject has been unreasonably withheld.

Where sensitive personal data is processed, a data controller must ensure that appropriate security safeguards are adopted. In addition, where genetic data and biometric data are processed for medicinal purposes and the consent of the data subject has been granted, such data is processed only if a unique patient identification number is given to the data subject.

Sensitive personal data which is processed may be provided to a third party only on the written consent of the data subject.

Processing of sensitive personal data for health or medical purposes

A health professional or other person who is subject to professional secrecy, may process sensitive personal data for health or medical purposes where this is necessary for (a) preventive medicine and the protection of public health; (b) medical diagnosis; (c) healthcare; or (d) the management of health and hospital care services.

Processing of sensitive personal data for research, scientific and statistical purposes

Sensitive personal data may be processed for research, scientific and statistical purposes without the consent of the data subject, provided that the processing is compatible with specified and legitimate purposes. A legitimate purpose is if (a) the Commissioner has approved the processing on the advice of a committee responsible for research and scientific ethics in an institution recognised by the Commissioner; and (b) the processing is necessary for statistical purposes as provided for under the Statistics Act.

Processing of an identity card number

A data subject's identity card number may, in the absence of the data subject's consent, be processed only where such processing is clearly justifiable, having regard to (a) the purpose of the processing; (b) the importance of a secure identification; or (c) any valid reason, as may be prescribed.

Special circumstances for processing sensitive personal data

A body of persons or an entity which has political, philosophical, religious or trade union objectives can process sensitive personal data, with appropriate guarantees. The Government of Botswana may process sensitive personal data for legal purposes where it is necessary for obtaining legal advice (e.g., in the management of a public health emergencies); to establish, exercise or defend legal rights; or for the administration of justice. Sensitive personal data may also be processed by the National Assembly, any government department or Ministry, on condition that it is necessary for exercising any function of the National Assembly, government department or Ministry, and that such processing is compatible with specified and legitimate purposes.

How personal and physical data can be construed as geospatial data

Geospatial data is not defined in the DPA. However, the definition of personal data in the DPA refers to information relating to an individual who can be identified or can be deemed to be identifiable through factors specific to that individual's physical data. Such physical data can be construed to include an individual's location or geospatial data – the individual's physical address or presence at a certain place in time. Geospatial data also qualifies as sensitive personal data

because it reveals a natural person's 'property details'. In addition, in certain circumstances, geospatial data can also be considered to be health data as it relates to the state of physical or mental health of an individual, collected for providing health services, or data which associates the individual with the provision of specific health services. For example, during a national health emergency or pandemic, the locations of individuals with an infectious disease may be collected for treating that person and to track and trace the whereabouts or geolocations of the people with whom such an individual has had contact with. This would enable governments and healthcare providers to manage health emergencies effectively. If geospatial data is collected and used as described above, the individual's consent for the processing thereof is not required, because such processing is carried out in the public interest.

Lawful processing of geospatial data where the health interest of the public or particular individuals is at stake

Consent is one of the legal grounds on which a data controller may process the sensitive personal data, including geospatial data, of an individual. Other legal grounds for the lawful processing of sensitive personal information include if the individual has made the data public; if the processing is necessary for national security; if the processing is necessary for any reason of substantial interest to the public; or if the processing is necessary to protect the vital interests of a data subject or another person and where neither the individual nor anyone on his or her behalf can provide consent. Geospatial data can, accordingly, be lawfully processed where the health interests of the public are at stake. During such times, lawful processing may also occur when the vital health interests of an infected or potentially infected individual are threatened.

Geospatial data could also be considered as a unique patient identification number where the patient's location is of vital importance for the management of an epidemic. In combination with the patient's ID, hospital or clinic number, this identification location may be unique – which requires the data controller to take appropriate security safeguards. A healthcare provider with a duty of confidentiality may process sensitive personal data for health or medical purposes where the processing is necessary for preventive medicine (such as vaccinations), the protection of public health (during an epidemic or pandemic), for medical diagnosis (in case of medical conditions that require the practitioner to report it as an infectious disease), healthcare (such as the treatment of

Covid-19 patients), or the management of health and hospital care services which may be triangulated during health emergencies.

Geospatial Data, SDIs and Public Health

The complete and accurate recording of any data relating to the health of any individual makes the difference between access to adequate healthcare or dying from treatable diseases. In this regard, geospatial data, specifically in the context of infectious disease pandemics, plays a similarly critical role. To fully understand this, the use of geospatial data as a tool for sustainable resource management and its role in the overall economic development of a country, in addition to its role in a public health context, must be understood. The underlying base for any decision-making in this regard depends on the development of spatial data infrastructures (SDIs), but there is confusion about the relationships among terms such as GIS and spatial data infrastructures. Clarification of these concepts is critical from a legal perspective in terms of deciding how to regulate these technologies and their impact on individual, societal and national levels.

General progress in SDI initiatives does not receive the necessary support from government, because of the low level of awareness of the importance of spatial data and information in decision-making. For this reason, GIS technologies and SDI initiatives remain innovative concepts among specific user communities. Resulting from this national lack of awareness of the value of SDI, there are also no policies or regulatory framework.

Geographic information is one of the most critical elements that underpins the analysis and decision-making for environmental, economic and social development. But considering how the land, space and environment that people live and work in affects their daily lives, lifestyles and health, GIS technologies and infrastructure must also be used to predict and manage public health.

Ehealth and Telemedicine Strategies

A critical assessment of the current draft eHealth strategy document suggests severe limitations. Botswana's draft 'eHealth' strategy lacks focus and would not be able to nurture, on its own,

innovative growth in the application of telemedicine initiatives which are currently fragmented and stalled. A specific Telemedicine Strategy that is properly aligned with and supportive of the more general eHealth strategy is necessary. If this proved to be the case for telemedicine, the effective implementation of geospatial information technologies in the health systems would also need to align with the eHealth strategy and requires a focused strategy of its own.

Conclusion and Recommendations

Botswana urgently needs an overall strategy with the buy-in and support of the national government to invest in the human and infrastructure resources necessary for the development, successful implementation and sustainable use of GIS-enabled technology for public healthcare. The management of such a strategy and the ultimate implementation of the related GIS technologies in the public healthcare context will dictate the regulations needed to regulate the effective, safe and secure use of geospatial data.

The regulation of geospatial data currently relies on the interpretation of the DPA, as discussed above.

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 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 the:

- Constitution of the Republic of Botswana
- Public Health Act

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 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 who 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 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, particularly by reference to an identification number, or to one 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	Personal data about a particular person which is considered sensitive, such as health data and genetic data, and which receives additional legal protection.

	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 proceedings; and (a) 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 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:

(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.)

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 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 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 thus 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 that 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, 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, particularly 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 Act. There is a special provision for the processing of personal data for research purposes in terms of the Act. However, the use of genetic data is restricted further and it can be processed only under the grounds in the 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 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 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 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 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 defense 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. The Commissioner may authorise a transfer of personal data to a third country that does not ensure an adequate level of security safeguards provided that 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.

LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE

This section develops/pioneers an approach to the legal regulation of artificial intelligence (AI) in health discovery and innovation. Data science in health research is increasingly used with AI applications that can transform health innovation. This requires robust governance, risk assessment strategies, and mechanisms to protect human rights

No AI legislation has been promulgated in Botswana. It is therefore necessary to consider the legal landscape associated with AI development and use. Five thematic areas considered most relevant to AI regulation are explored: (1) AI policy documents; (2) Digital/E-Health and medical device regulation; (3) Consumer/ICT legislation; (4) Data protection law; and (5) Intellectual property. These are discussed in turn below.

AI Strategy

Policy documents address the importance of AI for innovation and are discussed below. There is thus a 'wait and see' approach.

- *SMARTBOTS*: This is a digital transformation strategy aimed at building an internal market in the country, digitisation and innovation, competing globally, and building a knowledge workforce. Strategic initiatives include public sector transformation by ensuring universal connectivity, building digital skills to progress to a knowledge-based economy, and the establishment of the Maun Science Park - Living Lab, comprising a 4IR-enabled home community, research institution and an accelerator facility. Key projects include:
    - BotsRen: Educational and research institutions connected through networks
    - Digital Innovation Hub: A leader in public service transformation
    - Digital Literacy: Increasing ICT literacy to benefit from digital technologies
    - Open Data Resources: Data gathered under one roof for all to use
    - Science and Innovation School of Excellence (SISE) – to attract top students from across Africa.

- *Vision 2036*: Achieving Prosperity for All – With respect to information and communication technology the strategy will leverage ICT as a key contributor to economic growth and employment while also enabling an efficient private and public sector. An enabling environment, including digital access and the relevant regulatory framework, will be improved to enable the development of a private sector-led ICT industry.

- *National Development Plan (NDP) 11 Volume 1 April 2017–March 2023*: Current government data, network, data centre and information technology (IT) systems are inadequate, and do not adequately support efficient public service delivery. Similarly, government IT officers lack the skills to maintain and support the ICT infrastructure and services, therefore leading to slow uptake of new ICT initiatives and insufficient maintenance of existing systems and services. To address these issues, the NDP provides that the training of ICT personnel be prioritised in order to enhance the sector's contribution to economic and export diversification, and to create high-quality jobs. NDP 11 will attempt to achieve universal access to reliable high-speed networks in order to improve competitiveness and attractiveness to domestic and foreign investors, and the general public. Equitable and affordable access to broadband connectivity and services will fuel creativity and enable innovation among businesses and individuals by providing a platform that supports entrepreneurial advancement, access to information and services, and active citizen participation in the information society.

- *Smart Botswana*: As there will be a drive to develop smart cities globally, the country must catch up with the global community in order to follow suit. This will create an enabling environment that is conducive and competitive for doing business.

- *Secure Cyberspace*: The country's cyberspace will be secured to ensure customer confidence and to give confidence to investors to undertake business in the country. A National Cyber Security Strategy, which lays the foundational road maps for addressing national cyberspace challenges, was completed during NDP 10.

- *e-Services*: The ICT Policy recommends providing electronic services for economic growth and diversification. During NDP 11, the focus of public investment will be on the implementation of digitisation in different sectors of the economy, including e-Health, e-Education and e-Commerce. The private sector will also be enabled to offer electronic services through promulgation of laws and policies that are friendly to deployment of such services. Government will develop a digital data framework, providing a platform for open data. This will enable the use of much data generated by government and other service providers to generate new, relevant and local content, so creating efficiencies in the systems and leading to economic growth and new employment.

- *Research and Innovation Programme*: Aims to leverage research initiatives for realising economic value from indigenous knowledge.

- *2012 Research, Science, Technology and Innovation (RSTI) Policy*: The policy will integrate science and technology into all sectors of the economy and bring cohesion to fragmented research activities so that technology development, innovation and knowledge can drive national socioeconomic growth to transform Botswana into a globally competitive country. The Directorate will monitor the implementation of funded research projects, and develop and implement strategies and mechanisms for technology diffusion, uptake and transfer. It will also maintain a comprehensive RSTI data and information management system to inform decision-making.

- *Botswana E-Government Master Plan 2015–2021*: The strategy aims to: provide a blueprint for an effective e-Government programme; strengthen systems of e-governance to ensure sustainability; provide a coherent and holistic view of ICT strategies and initiatives; improve and maximise use of e-Government funds; and strengthen e-Government infrastructure. The core building blocks of e-Government include:
  - G2C: Improved access to information by reducing the digital divide and improving network speed in order to innovate civil services by providing information and improving access to information through ICT infrastructure growth.

- G2B: Enhanced competitiveness through economic diversification in order to innovate services to support business activities and provide the groundwork for collaboration with private networks.
- G2G: Innovating service delivery through seamless connectivity between government agencies in order to establish a foundation to support effective administration processes and the digitising of core government work.
- G2E: Providing meaningful opportunities through current and valid data in order to develop integration of employment data from the private and public sectors.
- Infrastructure: Providing realistic and relevant technologies to support e-Government programmes, in order to integrate and standardise information resources and establish effective management systems by introducing network infrastructure monitoring.

- *ICT Master Plan, 2012*: The strategy aims to transform the Parliament of Botswana by strengthening ICT governance and Parliament's information and knowledge infrastructure, and strengthening involvement in ICT policies and ICT for community development activities.

- *National Cybersecurity Strategy*: The strategy is premised on the core values of accountability, integrity, confidentiality and collaboration. Strategic objectives include:

  - Ensuring Botswana is more secure and resilient to cyberattacks by developing and reviewing appropriate policy, establishing an incident response team and security operation centre, protecting critical infrastructure, and developing national cyber contingency plans and capabilities to host national cybersecurity drills/exercises while continually monitoring cyber threats and risks.
  - Building a cybersecurity capacity and capability in Botswana by continually enhancing the resilience, integrity and trustworthiness of all networks and providing training that enhances capacities in cybercrime investigation and prosecution.
  - Promoting awareness of cybersecurity among the general public.
  - Fostering cybersecurity research and development.

- Enhancing collaboration and cooperation on cybersecurity issues at national, regional and international levels.
- Harnessing Botswana's cyberspace for socioeconomic development by raising cybersecurity awareness among decision-makers, policy-makers and political leaders and enhancing public–private partnerships to promote security and resilience in cyberspace infrastructure, networks, products and services.

Digital Health/E-Health

The eHealth Strategy of Botswana 2020–2024 governs digital health. It is complemented by the Botswana Health Data Collaborative Roadmap 2020–2025. The Botswana Health Professions Act, together with the Botswana Health Professions Council Code of Ethical Professional Conduct and the Botswana Health Professions Professional Conduct Regulations, regulate health professionals. Medical research is partially regulated by the Data Protection Act. The Medicinal and Related Substances Act defines medical devices but has not created formal processes for AI medical device regulation.

Consumer Protection & ICT/E-Legislation

Consumer protection	• Consumer Protection Act
ICT/E-legislation	• Communications Regulatory Authority Act • National Information and Communications Technology Policy • Electronic Communications and Transactions Act • Electronic Records (Evidence) Act • Financial Intelligence Act • The National Information and Communications Technology Policy (Maitlamo) has also been adopted to guide the development of ICT.

Data Protection Law

While no AI legislation has been developed, data protection law will heavily influence the uptake of AI systems in the country. The Data Protection Act is in force.

Relevant provisions

Relevant provisions include: rights to opt-out/opt-in; notice and consent requirements; minimum standards of data protection; and restrictions on off-shore data transfers. Botswana does not provide for a general prohibition on automated decision-making, as such provisions are unlikely to significantly affect the use of AI technologies.

Processing of sensitive data

There is a general prohibition on the processing of sensitive data. However, such processing is permitted if written consent has been obtained, the data subject has made the data public or where the processing is necessary for national security or performing rights or obligations under the law, or if authorisation is provided by any other written law, or for the protection of the vital interests of a data subject or another person. The data controller must ensure that appropriate safeguards are adopted. There are several exceptions to this general prohibition, including processing for health or medical purposes. Sensitive personal data may be processed if it is necessary for (a) preventative medicine and the protection of public health; (b) medical diagnosis; (c) healthcare; or (d) the management of health and hospital care services. With the processing of genetic and biometric data and where such data is processed for medicinal purposes with the consent of the data subject, a unique patient identification number must be given to the data subject.

Intellectual Property

Two pieces of legislation are relevant in this regard.

The Copyright and Neighbouring Rights Act

The Act provides for the protection of derivate works including collections of work and databases. However, no protection extends to any idea, procedure, system, method of operation, concept, principle, discovery or mere data, even if expressed, described, explained, illustrated or contained in a work.

Industrial Property Act

The Act does not define an 'inventor' and an application for a patent in respect of an invention may be made by the inventor or by any other person who has acquired the right to apply from the inventor.

Summary and Analysis

As there is no dedicated AI legislation, it is necessary to consider the legal landscape associated with AI development and use.

While several ICT policy documents that support 4IR enablement have been produced, relevant provisions in legislation take precedence. The policy documents are interoperable and do not supersede one another. These documents envision digital transformation across Botswana by leveraging information and communication technology. Focus areas include strengthening ICT infrastructure, increasing research and innovation, providing e-services, and developing a cybersecurity framework. New regulatory developments such as the Smartbots policy and National Cybersecurity Strategy are vital for ensuring that practical steps are taken to encourage the responsible development and use of AI-based technologies. While there are several policy documents to guide digital heath implementation, Botswana is yet to develop a formal medical device registration process.

Within the legal framework for data protection, restrictions on the processing of personal data are particularly important for health research. Unfortunately, Botswana's data protection legislation does not have a specific provision on automated decision-making. Those purchasing AI technologies are unlikely to find much protection under the Consumer Protection Act. However, ICT/E-legislation such as the Electronic Communications and Transactions Act and a consideration of intellectual property legislation, jurisprudence and soft law may be critical in ensuring that these technologies are used properly.