KENYA

ACRONYMS

4IR	Fourth Industrial Revolution
AI	Artificial intelligence
ALC	African leadership conference
ARMC	African Resource and Environmental Management satellite Constellation
DPA	Data Protection Act
GDPR	General Data Protection Regulation (Europe)
ICT	Information and communication technology
IPR	Intellectual property rights
KSA	Kenya Space Agency
MIDST	Monitoring for Information and Decisions using Space Technology
NACOSTI	National Commission for Science and Technology
NSP	National Space Policy
PI	Principal investigator
SKA	Square Kilometre Array
UNOOSA	United Nations Office for Outer Space Affairs

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 National Commission for Science and Technology (NACOSTI) National Guideline and the Data Protection Act (2019) are the main regulatory instruments.

NACOSTI's National Guideline for Ethical Conduct of Biomedical Research Involving Human Participants in Kenya

Under the NACOSTI National Guideline, researchers must obtain voluntary written informed consent from research participants and required information must be provided to a participant in simple language. Consent from individuals is still required where there is a community agreement or consent from a community leader to engage in research. Reconsenting is encouraged when considering secondary use of biological materials or data. However, a research ethics committee may waive the requirement of consent if the data or material is delinked from personal identifiers.

Data Protection Act

For processing personal data, the Data Protection Act is also applicable. Specific informed consent applies. The Act requires that before processing personal data, the consent of the data subject must be obtained. There are, however, some exceptions, including if the processing is necessary for scientific research.

Genetic data and sensitive personal data

Genetic data is classified under sensitive personal data. Under the Act, sensitive personal data means data revealing or related to the natural person's race, health status, ethnic social origin,

conscience, belief, *genetic data*, biometric data, property details, marital status, family details, sex or sexual orientation.

Data subject physically or legally incapable of giving consent

Where a data subject is physically or legally incapable of giving consent, the processing of data will be allowed if necessary to protect the vital interests of the data subject or another person.

Withdrawal of consent

The data subject can withdraw his or her consent at any time but this will not affect the lawfulness of processing based on prior consent before the withdrawal.

Transfer of data outside Kenya

To transfer of data outside Kenya, apart from obtaining confirmation of appropriate safeguards, the consent of the data subject is also required. However, this requirement can be exempted in relation to scientific research.

Data Protection Regulations

According to the Data Protection (Registration of Data Controllers and Data Processors) Regulations, before informed consent is obtained for data collection, the data subject should be informed of the following:

- the identity of the data controller or data processor;
- the purpose of each of the processing operations for which consent is sought;
- the type of personal data that is collected and used;
- information about the use of the personal data for automated decision-making, where relevant;
- the possible risks of data transfers as a result of absence of an adequacy decision or appropriate safeguards;
- whether the personal data processed will be shared with third parties;
- the right to withdraw consent; and

- the implications of providing, withholding, or withdrawing consent.

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.

A number of rights relevant to human genomics research are protected. The Constitution protects privacy, freedom of expression and the right to academic freedom and freedom of scientific research, among other rights. These rights are properly outlined and implemented in legislation, regulations and policy guidelines.

Regulatory and Supporting Institutions

Several institutions are involved in regulating and supporting compliance with human genomic research. These include the:

- Bioethics Society of Kenya
- Kenya Institute for Public Policy Research and Analysis
- Kenya Medical Research Institute
- Kenya National Innovation Agency
- Ministry of Health
- National Commission for Science, Technology and Innovation
- Office of the Data Protection Commissioner
- Pharmacy and Poisons Board Kenya.

Individual and Community Benefit Sharing

The approach to benefit sharing is as follows. With respect to research on human participants, it has to be collaborative between the investigators and local researchers. Benefit sharing must be

included in the research proposal and thus community benefit sharing is conducted in terms of local training, technology transfer, improvement of healthcare, and information infrastructure. The potential benefits must be disclosed and where the biological sample is genome sequenced, then such should be included in the consent document with information on the participant's whole genome determined through scientific tests; information to the effect that the research participant's whole genomic sequence is unique to him/her; and where secondary use of the biological material or data is likely, the consent document must clearly explain how this will occur, with whom the material or data will be shared, and how consent and identification will work.

Benefits

(1) Tissue donation, removal and associated payment

For any tissue, organ, blood or gametes to be removed from any person, that person must give written consent and it must take place in a authorised medical facility. Consent can be given during a person's lifetime for his body organ or tissue to be used for a specified purpose after death through a will or consent to post-mortem examination of his/her body. A person can also consent to his/her tissue, organ, blood or gametes being removed while still living. All forms of consent for biomedical research must be written and community consent cannot be a substitute for individual consent. Consent to donate must include a statement about the study, recruitment procedures, benefits, risks, compensation, voluntariness, confidentiality statement, and researchers.

Organs, tissues, blood, blood products, and gametes cannot be sold. The donor is not entitled to receive any payment for donating organs, tissues, blood, blood products, or gametes. However, the donor can receive compensation for costs incurred in the process of making the donation or injuries sustained in the cause of the research activities. The amount reimbursed or given as compensation for costs incurred or injuries sustained thus covers costs only.

Purpose is limited to:

- the purposes of training of students in the health sciences
- the purposes of health research
- the purposes of the advancement of health sciences
- therapeutic purposes, including the use of tissue in any living person
- the production of a therapeutic, diagnostic or prophylactic substance.

(2) Patenting

Patenting is generally allowed. However, several inventions cannot be patented:

- discoveries, scientific theories and mathematical methods;
- schemes, rules or methods for doing business, performing purely mental acts, or playing games;
- methods for treating the human or animal body by surgery or therapy and diagnostic methods practised in relation to that, except products for use in any such methods;
- mere presentation of information;
- public health-related methods of use or uses of any molecule or other substance used for the prevention or treatment of any disease which may be classified as a serious health hazard or as a life-threatening disease;
- inventions contrary to public order, morality, public health and safety, and principles of humanity and environmental conservation.

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.

There are no laws, guidelines, or policies in Kenya that specifically provide for the regulation of geospatial data. In this context there has to be reliance on laws pertaining to data protection in general.

Pertinent legislation, regulations, guidelines and policies are discussed below.

General Framework

Legislation

The Data Protection Act (DPA)

The DPA refers to personal data as any information relating to an identified or identifiable natural person. The term "identifiable natural person" means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This definition encompasses various types of data, including location data, and thus geospatial data must be treated as personal data when it can be linked to an individual.

Consent

If geospatial data is collected and processed in a manner that can identify individuals (e.g., through location-based information), the principles of lawful data processing outlined in the DPA apply. Data controllers are generally required to obtain the consent of data subjects before collecting and processing their geospatial data. Consent should be express, informed, freely given, and revocable.

Where processing is necessary for purposes of scientific research it may be processed without consent, save for sensitive data where special restrictions apply and where additional safeguards are required.

Purpose limitation

Geospatial data collected must adhere to the principle of purpose limitation. Therefore, the data should be collected and processed only for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes. The DPA includes a 'data protection by design' provision. The DPA requires a data controller or data processor to implement appropriate technical and organisational measures to ensure that only personal data which is necessary for each specific purpose is processed. Data controllers should not use geospatial data that identifies individuals for purposes other than what was initially stated or agreed upon, without obtaining additional consent.

Data security

The DPA requires data controllers to implement appropriate technical and organisational measures to safeguard personal data from all external and internal risks, which may include unauthorised access, disclosure, or destruction. Security measures must ensure the confidentiality, integrity and availability of the data.

Data subject rights

These include the right to access geospatial data held by data controllers, the right to rectify inaccurate data, and the right to request the deletion or erasure of data under certain circumstances.

Cross-border data transfer

If geospatial data is transferred to countries or organisations outside Kenya, the DPA requires that the data controller or data processor give proof to the Data Commissioner that adequate safeguards are in place to protect the data during such transfers and that appropriate safeguards are also in place for jurisdictions with commensurate data protection laws.

Sensitive personal data

Sensitive personal data is defined as data revealing (information about) the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details, parents, spouse/s, sex or sexual orientation. The inclusion of property details in the DPA may make the additional special protections afforded to sensitive data applicable to geospatial data that identifies an individual in relation to his/her property details.

The DPA make provision for sensitive personal data to be treated differently. There are grounds/conditions and restrictions for processing such data. The general principles for how personal data should be treated deal with issues such as:

- privacy of the data subject;
- data to be used for a specified purpose;
- data that is incorrect should be swiftly rectified or deleted; and
- there must be proof of adequate safeguards or consent from the data subject for cross-border transfer of the data.

There are restricted grounds on which sensitive data may be processed without express consent, and those grounds do not include a general exemption for scientific research. There is a stricter approach to how sensitive personal data is protected in the DPA compared to other personal data. There is, however, an exemption in the Data Protection Regulations (discussed below) for the collection, use or disclosure of health data for health research and related purposes without express consent, which can be regarded as being in the public interest. The DPA mentions public interest in the area of public health as a ground for processing health data as follows:

> (1) Personal data relating to the health of a data subject may only be processed —
> (a) by or under the responsibility of a healthcare provider; or
> (b) by a person subject to the obligation of professional secrecy under any law.
> (2) The condition under (1) is met if the processing —
> (a) is *necessary for reasons of public interest in the area of public health*; or
> (b) is carried out by another person who in the circumstances owes a duty of confidentiality under any law.

Health data is defined as data relating to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of health, 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.

Genetic data is mentioned under the definition of sensitive personal information in the DPA. The DPA defines biometrics as 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.

These considerations warrant attention by health researchers combining geospatial data with health data in such a way that individuals may be identifiable.

Enforcement and penalties

The DPA outlines penalties for violations, including fines and imprisonment for individuals or organisations found to be in breach of the law. The Data Commissioner's Office is responsible for enforcing the DPA. When geospatial data, like other forms of personal data, is subject to the provisions of the DPA in Kenya, the DPA requires data controllers to handle personal data responsibly, with explicit consent, to secure storage and processing, to adhere to the principle of purpose limitation, and with respect for data subject rights. Where an individual is identifiable from geospatial data, compliance with these regulations is crucial to protect the privacy and rights of individuals whose geospatial data is being collected and processed.

Regulations

The Data Protection (General) Regulations

The Regulations state that the collection of personal data entails obtaining personal data directly from a data subject or by any means, including from:

(a) any other person;

(b) generally available publications or databases;

(c) surveillance cameras, where an individual is identifiable or reasonably identifiable;

(d) information associated with web browsing, including personal information collected by cookies; and

(e) biometric technology, such as voice or facial recognition.

All sources of geospatial data where an individual is identifiable from the data would be covered. For health researchers, the Regulations provide a significant public interest exemption from the requirement for express consent. This is important in cases of monitoring and predicting disease outbreaks. The Regulations state:

A permitted health situation exists in relation to the collection, use or disclosure by a data controller or data processor of personal data about a data subject, including for –

(a) the collection of health information to provide a health service;

(b) the collection, use, or disclosure of health data for health research and related purposes;

(c) the use or disclosure of genetic information if necessary and obtained in the course of providing a health service;

(d) the disclosure of health information for a secondary purpose to a responsible person for a data subject.

Guidelines

National Spatial Plan

The National Spatial Plan and National Land Use Policy provide the framework and vision that guide the long-term spatial development of Kenya. The Plan addresses uncoordinated human settlements, disjointed sectoral policies, urban and rural development, economic development disparities, unsustainable use of the natural environment, and inefficient transport and infrastructure.

National Land Commission County Spatial Plans, 2015

These guidelines provide a basis for engagement between the county governments as planning authorities responsible for preparing, approving, and implementing County Spatial Plans and the National Land Commission as a monitoring and oversight agency over land-use planning.

The County Government Act stipulates that the County Spatial Plans must give effect to the principles and objects of county planning and development. Furthermore, the County Spatial Plans should set out basic guidelines for a land-use management system in the county considering any guidelines, regulations or laws as provided for under the Constitution. The Constitution provides that every person has the right to a clean and healthy environment and to the highest attainable standard of health, which includes the right to healthcare services, including reproductive healthcare. This suggests that the Constitution allows for a health environment that directly influences the start, spread and management of health epidemics which may affect or relate to geospatial data. This is because if one can establish where people live and what segment of the population they are, one can better manage their healthcare needs.

The guidelines guide and standardise the preparing and implementing of County Spatial Plans. The County Spatial Plan is an instrument for realising constitutional promises and expectations. This includes regulation of land use and property in the interest of defence, public safety, order, morality, *public health* or land-use planning. One of the themes covered by the situational analysis is social development. This entails population and *demographic characteristics***,** *health*, education, other social amenities, and socio-cultural issues.

The County Spatial Plans show that one of their expected impacts is improved access to infrastructure and services. This includes schools, health facilities, and recreation facilities. This is an important managerial aspect when managing an epidemic. Personal geospatial data then becomes important for mapping the proximity of people to hospitals.

Policies

Kenya National eHealth Policy 2016–2030

This deals with Equitable Access to Quality Healthcare Services Using ICTs. The adoption of eHealth as a model of care will help mitigate health inequalities that result from differences in the social and economic conditions across geographical and political boundaries. The healthcare services and information provided through eHealth should be of good quality. The Policy also mentions that a certification body needs to be set up to perform annual surveillance audits and periodic assessment audits to proactively verify that certified eHealth owners or companies comply with legal and policy requirements.

National Land Use Policy

The Policy describes land use in Kenya and mentions how urbanisation and the concentration of people in certain areas can affect public healthcare.

National Space Policy

The National Space Policy (NSP) was developed against the backdrop of Kenya's Vision 2030 goal to become a middle-income country by 2030. Space science and technology have been recognised in the NSP as a critical pillar in several socioeconomic goals including telemedicine, and using space technology to take health services to remote parts of the country. The Kenya Space Agency (KSA) together with the United Nations Office for Outer Space Affairs (UNOOSA) held a Technical Advisory Mission on Space Law as a precursor to developing a Space Bill for Kenya.

Project MIDST (Monitoring for Information and Decisions using Space Technology)

Project MIDST was launched to use new and advancing geospatial technologies for government decision-making in natural resource management (forests), spatial planning (urbanisation), and disaster management (floods/landslides).

Multilateral Centre for Space Science and Technology Education in Africa

Kenya is a participant in the Multilateral Centre for Space Science and Technology Education in Africa, and is engaged in the promotion of bilateral and multilateral relations with institutions participating in space activities from other countries.

Possibilities beyond our skies: Strategic plan 2020–2025

The KSA developed 'Possibilities beyond our skies: Strategic plan 2020–2025', in which universal health coverage is identified as a priority application. Space applications will support spatial mapping of health coverage, health facilities and identify underserved areas to inform resource allocation. Besides supporting epidemiology of infectious diseases and monitoring health risks and disease patterns to inform disease-control planning and interventions, other applications such as telecommunications technologies enable sharing of health resources, including expertise through virtual contact with patients and health practitioners, including remote, rural and underserviced areas through tele-health, tele-medicine and needs analysis. The strategic plan outlines several initiatives, of which the improvement of the satellite communications programme is vital for disease monitoring and telemedicine.

Relevant International Conventions and Treaties

Kenya subscribes to the international conventions and treaties on peaceful uses of outer space and actively participates in the

- African leadership conference on Space Science Technology for Sustainable Development (ALC)
- African Resource and Environmental Management satellite Constellation (ARMC) initiative
- Square Kilometre Array (SKA) programme.

Kenya signed the 1976 Bogota Declaration on management of the equator and geostationary orbit as national resources.

Kenya's space activities are sectorally placed in a number of government agencies and institutions that play a key role in the use of space applications.

Conclusion and Recommendations

Kenya has developed a strong legal framework for data protection, and has implemented policies governing e-Health, space, and land use and spatial planning. However, infrastructure and implementation of geospatial data in healthcare applications remains suboptimal.

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 personal data is governed by several laws and regulations, which must be carefully considered and complied with before researchers share data for research purposes. In Kenya, the Data Protection Act is in force. It is a general data protection law that applies to the processing (i.e., use) of personal data in all sectors. While it is not a statute introduced specifically to regulate research, it applies to research that involves the processing of

personal data. It is only one of several laws that must be complied with when transferring personal data for research purposes.

Health Research Regulations Involving Human Participants and Cross-Border Data Sharing

In addition to the national laws listed below, several international treaties and conventions have been signed. However, Kenya has not yet ratified the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention).

The relevant national health legislation is the National Health Act of Kenya and the Science Technology and Innovation Act. Numerous policies, regulations and guidelines have been made in terms of the Science Technology and Innovation Act, including:

- Ethical Guidelines for Public Health Emergencies in the Response to Covid-19 Pandemic in Kenya, 2020
- Guidelines for Accreditation of Institutional Ethics Review Committees in Kenya, 2017
- National Guidelines for Ethical Conduct of Biomedical Research Involving Human Participants in Kenya, 2020
- National Guidelines for Registration of Research Institutions in Kenya, 2020
- National Guidelines for Registration, Licensing, and Regulation of Researchers in Kenya, 2022
- Science, Technology and Innovation Policy 2020–2030

These laws, policies, regulations and guidelines set out the legal and ethical requirements that must be met for the conduct of research in Kenya and must be complied with when data is being transferred across borders.

International collaborative research requires the involvement of a Kenyan PI.

Data Protection Act

In addition to these legal and ethical requirements, the Data Protection Act and the Data Protection General Regulations apply to the processing of all personal data, but in acknowledging the importance of research, special provisions are in place that deal with the processing of personal data for research purposes.

Personal data that is processed for research purposes only is exempt from the provisions of the Act if: it is processed in compliance with the relevant conditions; and results of the research or resulting statistics are not made available in a form which identifies the data subject. This means that the relevant provisions of the Act for research must be complied with and research results and research stats cannot be made available in a form that identifies the data subject.

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 Act are listed and 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 identified or identifiable natural person who is the subject of personal data.	The person to whom the data relates.
Data controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.	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 natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.	Someone who is not directly employed by the data controller but who processes personal data under the direction of the data controller.

		The person may be a consultant, for example.
Data Commissioner	The person appointed under the DPA.	The independent body established to monitor and enforce compliance with the law.
Data Protection Officer	Not defined in the Act. However, the person is appointed in terms of the DPA.	An individual in an organisation who is appointed to advise and to promote compliance with the law.
Identifiable natural person	A person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.	
Third party	Natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.	

Categories of Data Listed in the Data Protection Act

	Legal definition	**Layman explanation**
Personal data	Any information relating to an identified or identifiable natural person.	Data about a particular person that can identify him or her.
Sensitive personal data	Data revealing the natural person's race; health status; ethnic social origin; conscience; belief; genetic data; biometric data; property details; marital status; family details including names of the person's children, parents, spouse or spouses; sex; and sexual orientation.	Personal data about a particular person which is considered sensitive, such as health data and genetic data, and which receives additional legal protection.

Pseudonymisation	The processing of personal data such that it can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.	Data where the direct identifiers have been removed (e.g., a name) so that it is impossible to identify the person without adding other information. This is often called coded data. Data protection law still applies to pseudonymised data.
Anonymous data	Not defined.	Data where it is no longer possible to identify a person from the data. It must not be possible to re-identify the person. Data protection law does not apply to anonymised data.
Anonymisation	The removal of personal identifiers from personal data so that the data subject is no longer identifiable.	

While data protection law does not usually apply to anonymised data, neither Kenya's Data Protection Act nor its Regulations explicitly exclude anonymised data from the ambit of their provisions. According to the Act, anonymisation means "the removal of personal identifiers from personal data so that the data subject is no longer identifiable". The Act provides that data must be anonymised in a way that ensures "the data subject is no longer identifiable". Unfortunately, the Act and the Regulations do not contain standards for non-identifiability. While the test for anonymisation remains elusive, Kenya's Data Protection Act clearly applies only to the processing of personal data, and therefore data which has truly been rendered no longer individually identifiable – i.e., anonymised – will presumably fall outside its ambit.

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.

There is some uncertainty about from whose perspective the data must be considered anonymised.

On this there are two possibilities:

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

The first test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to 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.

In the absence of direction from the Commissioner on a test, the data controller will have to decide. In making this decision, general points may be worth keeping in mind (many of which come from guidance related to anonymisation under the GDPR):

- An assessment must be made on a case-by-case basis, considering the particular context.
- The anonymisation must be irreversible.
- The assessment is made on the current state of the art. As technology progresses, data that was once deemed to be anonymous may become personal data and thus 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, particularly 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 by Every Data Controller or Data Processor in Terms of the Data Protection Act

1. *Data must be processed in accordance with the right to privacy of the data subject:* Personal data should be processed such that it ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Both organisational and technical measures must be put in place to secure the data.
2. *Data must be processed lawfully, fairly and transparently in relation to any data subject:* Personal data must be processed lawfully, fairly, and transparently in relation to the data subject. Lawful means that there must be a legal basis for the processing of the personal data as set out in the Act. The processing of sensitive personal data is generally not permitted unless it falls within one of the grounds as set out in the Act.
3. *Data must be collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes:* Personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that the purpose must be clearly set out.

4. *Data collected must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed:* Only the data necessary for the specific purpose should be collected and processed. Only the minimum amount of data required to achieve the objectives of the data processing must be used. The data can be further processed if it is used for historical, research or statistical purposes. The data controller or data processor would have to ensure that the further processing of data is carried out solely for such purposes and that it will not be published in an identifiable form. Personal data processed for research purposes is exempt from the provisions of the Act if it is processed in compliance with the relevant conditions. Furthermore, if the results of the research or statistics are not available in a form that identifies the data subject, then personal data is exempt.
5. *The data must be accurate and, where necessary, kept up to date, with every reasonable step taken to ensure that any inaccurate personal data is erased or rectified without delay:* Personal data must be accurate and, where necessary, kept up to date. Processes should be in place to ensure that all personal data collected is accurate.
6. *The data must be kept in a form that identifies the data subject for no longer than is necessary for the purposes for which it was collected:* Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Once the objective of the processing has been achieved, the data should be deleted. Data that is rendered anonymous does not fall under data protection law. However, to anonymise the data, there must still be a lawful basis to do so.
7. *Data should not be transferred outside Kenya unless there is proof of adequate data protection safeguards or consent from the data subject:* Personal data may only be transferred to another country after receipt of proof to the Data Commissioner on appropriate safeguards in respect of the security and protection of the personal data and this includes jurisdictions with commensurate data protection laws. The transfer must also be necessary for any matter of public interest. In relation to sensitive personal data, consent from the data subject and obtaining confirmation of appropriate safeguards is required, among other things.

Data Subject Rights in Terms of the Data Protection Act

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

1. *Right to be informed about how their personal data will be used:* The data subject has the right to be informed about what his/her personal data will be used for.
2. *Right to access their personal data in the custody of the data controller or data processor:* The data subject has the right to access personal data that the data controller has about them. The data controller should have a process in place to facilitate this.
3. *Right to object to the processing of all or part of their personal data.*
4. *Right to rectification of false or misleading data:* The data subject has the right to have inaccurate personal data corrected and incomplete data to be completed.
5. *Right to the erasure of false or misleading data about them:* The data subject has the right to request that their data be erased.
6. *Right to restriction of processing:* The data subject can request that the data controller stop processing his/her personal data.
7. *Right to data portability:* The data subject has the right to move his/her data from one data controller to another.
8. *Right to object to the processing of all or part of their personal data:* The data subject can object to the processing of his/her personal data where the lawful basis of processing is not consent.
9. *Right to object to automated individual decision-making:* The data subject has the right to object to a decision based solely on automated processing.

Cross-Border Sharing of Personal Data

Each of the provisions applies to any research that uses personal data. Data protection law also has additional provisions that must be met when personal data is to be transferred outside of the country. These additional provisions are in place to ensure that data subjects continue to be protected once the data leaves the country.

While cross-border data sharing is not defined in data protection law, the laws on cross-border data sharing apply to information sent to a data controller in another country. It *could* also include where a researcher outside of the country accesses personal data in the country. It *could* also include putting data onto a cloud where the server is not hosted in the country. Whether it does apply in these contexts is still not settled law.

In addition, there must be a ground under which the transfer can occur.

***Legal bases* for transferring personal data out of Kenya in terms of Data Protection Act**

1. The data controller or processor provides the Data Commissioner with evidence of appropriate safeguards with respect to the security and protection of personal data.
2. Transfer is necessary for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request.
3. Transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another person.
4. Transfer is necessary for any matter of public interest.
5. Transfer is necessary for the establishment, exercise or defence of a legal claim.
6. Transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
7. Transfer is necessary for compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

Cross-Border Sharing of Sensitive Personal Data

The cross-border sharing of sensitive personal data out of Kenya is permissible only if the data subject has consented and there are appropriate safeguards.

If sensitive personal data can be shared on this ground, the Data Commissioner may request a demonstration of the effectiveness of the security safeguards or the existence of compelling

legitimate interests. It is therefore good practice for researchers to keep a record of these safeguards or interests.

The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfers to such conditions as may be determined.

The Cabinet Secretary may prescribe a certain nature of processing that may be effected only through a server or data centre located in Kenya based on the grounds of the strategic interests of the state or protection of revenue.

LEGAL REGULATION OF AI

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

There is no specific AI legislation in Kenya. Therefore, it is necessary to consider the legal landscape of 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.

AI Strategy

Several sector/industry-specific policy documents treat the potential of AI development and use: the National Broadband Strategy, 2018–2023; National Information, Communications and Technology (ICT) Policy, 2019; and the Digital Economy Strategy – Draft 2, 2020. The most significant contributions to AI regulation include:

- The *Digital Economy Blueprint, 2019* considers AI to be an emerging trend and provides a general methodology for governments addressing emerging technologies to safeguard the benefiting communities and drive digital business and government in a locally relevant way. This requires considering the implementation of: adaptive regulation, regulatory sandboxes, outcome-based regulation, risk-weighted regulation, and collaborative regulation.

- *Emerging Digital Technologies for Kenya: Exploration and Analysis, 2019* is a critical and contextual review of emerging technologies. The taskforce considered the role of digital technologies in delivering the government's Big Four Agenda of affordable housing, universal healthcare, manufacturing and food security, and have also provided a roadmap

for the implementation of blockchain and AI technologies in Kenya and the manner in which these technologies can promote and enhance government services. AI's value is understood to lie in its ability to provide enhanced data analytics, provide better informed decision-making, improve predictive analysis, improve private sector profitability and potentially increase national competitiveness by accelerating the rate of innovation. Challenges to regulation include: a consideration of how to balance innovation and competition as well as the transnational nature of AI and the national character of laws. The report identifies unemployment, infringement of privacy, unethical AI applications and 'weaponisation' as key risks in the effective and inclusive implementation of AI technology. The taskforce recognises that these risks may be mitigated by skills development and local research and development initiatives. However, the short supply of local public data poses difficulties.

In considering Kenya's regulatory approach to AI, the taskforce notes that: Three key activities should be analysed when considering the regulation, use and supportive development of AI solutions in a country:

(1) Develop supportive policies to enable short- and long-term use of AI by analysing existing policies and creating new policies to ensure that citizens' rights are protected. AI requires large amounts of centralised data to function effectively. However, centralising such large amounts of data can pose a risk to privacy if effective policies on access, use, ownership and control of data by a third party (which could be a government) are not implemented.
(2) Create an effective ecosystem to support, manage and grow AI solutions, including infrastructure, skills development and cross-sector linkages. AI operates most effectively when it has access to large amounts of data, which also requires supportive infrastructure (increasing connectivity and improving data collection mechanisms) and interoperability through cross-sector linkages. Effective and inclusive skills development is also required to create and manage AI solutions to mitigate the risk of AI programmes with hardcoded biases, which can result in unethical AI.

(3) Manage and analyse the potential long-term effects of AI and develop systems to manage these risks early in the implementation. For example, one of the most discussed risks is the unemployment that occurs when tasks previously performed by humans are performed by AI systems. If a country does not effectively analyse and manage this risk prior to its occurrence, the social welfare system could easily become crippled by unmanageable unemployment. Emerging digital jobs could be tracked globally, and countries could develop effective training programmes to re-skill citizens at high risk of unemployment.

In the healthcare sector, AI can mitigate the shortage of healthcare workers in developing countries by using AI in clinical decisions – specifically patient triaging, diagnosis and decision-making. Then health professionals can focus on more advanced medical tasks. AI is also useful in disease control.

Much as in other sectors, data is seen as a key enabler for AI in healthcare. The taskforce therefore recognises the need for a large exercise to collect useful data from, for example, personal monitoring devices and electronic health records. The taskforce asserts that a first step would be to digitise all patient/medical records to realise easier access to and updating of records to generate the required datasets. It is believed that accurate data collection and verified data can help deliver healthcare effectively through, for example, patient monitoring/tracking, drug monitoring/tracking, cost control, predictive care, and remote care.

Digital Health/e-Health

The Kenya National e-Health Policy 2016–2030 guides digital health. The National Community Health Digitization Strategy 2020–2025, Standards and Guidelines for Health systems 2017 and the Tele-Mental Health Guidelines 2021 complement the e-Health policy. The Kenya Information Communication Act has provisions that regulate telemedicine in healthcare. There is also a standalone E-health Bill that regulates digital health. The Medical Practitioners and Dentist Act and the Code of Professional Conduct and Discipline regulate health professionals. No legislation

defines AI as a medical device or software as a medical device explicitly. However, the definition of a medical device in the Pharmacy and Poison Act includes software as a medical device. Ostensibly, this also covers AI in healthcare. Medical research is regulated by the Pharmacy and Poison Act.

Consumer Protection/E-legislation

Consumer Protection	• Consumer Protection Act
ICT/E-legislation	• Kenya Information and Communications Act • Access to Information Act

Data Protection Law

While no AI-specific legislation has been developed, data protection law will heavily influence the uptake of AI systems in the country. The Data Protection Act covers both public and private sector processing of personal data. Relevant provisions include those relating to minimum standards of data protection. Data is to be

(1) used only for the specified purpose for which it was originally collected
(2) adequate, relevant and not excessive to purpose
(3) accurate and up-to-date
(4) accessible to the data subject
(5) kept secure
(6) destroyed after its purpose is completed.

There are restrictions on the processing of sensitive (health/genomic) data, and a general prohibition on automated decision-making and data protection by design or by default.

The Act considers grounds for processing sensitive personal data. Such processing must not be undertaken, with certain exceptions. These include instances in which processing is: carried out by a non-profit body; and in relation to personal data made public by the data subject or necessary for establishing, exercising or defending a legal claim, carrying out the obligations and exercising

specific rights of the data controller or of the data subject or protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent. Personal data relating to the health of the data subject may be processed only by a healthcare provider or individual subject to professional secrecy if such processing is necessary for the public interest in the area of public health law or is carried out by another person who has a duty of confidentiality under any law.

There is a general prohibition on automated decision-making, except in instances in which the decision is: necessary in relation to a contract between the data subject and data controller, and authorised by a law which provides for suitable safeguards or based on the data subject's consent. Where such automated decision-making occurs, the data controller or data processor must notify the data subject who may in turn request that the decision be reconsidered or that a new decision that is not based solely on automated processing be taken. On receipt of such a request, the data controller or data processor must consider the request, comply with the request and inform the data subject of the steps taken to comply – as well as the outcome of complying with the request. The Cabinet Secretary can create regulations to provide further suitable safeguards.

The Act provides for data protection by design/default. Data controllers must implement appropriate technical and organisational safeguards aimed at ensuring that only personal data which is necessary for each specific purpose is processed. Determining the necessity of personal data will depend on the amount of data, extent and cost of processing, storage period, accessibility and the technology and tools used in processing. The data controller should consider appropriate measures such as: identifying reasonably foreseeable risks and subsequently developing, verifying and continually updating safeguards, pseudonymising or encrypting personal data, and timeously restoring access to data after an unforeseen incident. The data controller should consider the state of tech development, cost of security measures, special risks of processing, and the nature of the data itself.

Several regulations guide the enforcement of data protection in Kenya. These are the

- Data Protection (Civil Registration) Regulations

- Data Protection (Complaints Handling and Enforcement Procedures) Regulations
- Data Protection (Compliance and Enforcement) Regulations
- Data Protection (General) Regulations
- Data Protection (Registration of Data Controllers and Data Processors) Regulations.

Intellectual Property

Constitution of Kenya

Importantly, intellectual property rights (IPR) are recognised in Kenya's Constitution. First, 'property' is defined as including IPR and the state must support, promote and protect the IPR of the people of Kenya. In terms of obligations in respect of the environment, the state must protect and enhance intellectual property in, and indigenous knowledge of, biodiversity and the genetic resources of the communities.

Industrial Property Act

The Industrial Property Act defines 'inventor' as 'the person who actually devises the invention and includes the legal representative of the inventor.

An 'invention' is defined as a new and useful art (producing a physical effect or not), process, machine, manufacture or composition of matter which is not obvious, or any new and useful improvement which is not obvious, capable of being used or applied in trade or industry, and this includes an alleged invention.

Copyright Act

Relevant definitions include:

(1) 'author', in relation to—

(a) a literary, musical or artistic work means the person who first makes or creates the work;

(g) a literary, dramatic, musical or artistic work or computer program which is computer generated, means the person by whom the arrangements necessary for the creation of the work were undertaken; and

(h) a computer programmer means the person who exercised control over the working of the program.

(2) 'computer' means an electronic or similar device with information-processing capabilities.

(3) 'computer program' means a set of instructions expressed in words, codes, schemes or in any other form, which can, when incorporated in a medium that the computer can read, cause a computer to perform or achieve a particular task or result.

(4) 'literary work' means, irrespective of literary quality, any of the following: (a) novels, stories and poetic works; (b) plays, stage directions, film sceneries and broadcasting scripts; (c) textbooks, treatises, histories, biographies, essays and articles; (d) encyclopaedias and dictionaries; (e) letters, reports and memoranda; (f) lectures, addresses and sermons; (g) charts and tables; (h) computer programs; and (i) tables and compilations of data including tables and compilations of data stored in a computer or a medium used in conjunction with a computer.

Summary and Analysis

While several ICT policy documents that support 4IR enablement have been produced, relevant provisions in legislation take precedence over other regulatory/policy documents. The above-mentioned policy documents are interoperable and do not supersede one another. These documents envision digital transformation across Kenya by leveraging information and communication technology. Focus areas include strengthening ICT, broadband and data infrastructure, as well as the use of AI technologies to achieve Kenya's Big 4 Agenda, which includes the provision of universal health. the Digital Economy Blueprint and Emerging Technologies Strategy both address AI regulation. While there are several policy documents that guide digital health implementation, new regulatory developments such as the E-health Bill 2021 are vital in ensuring regulation of these technologies used in the healthcare sector. In addition, the inclusion of software in the definition of medical devices suggests at least some level of regulatory control/oversight over these technologies.

Within the legal framework for data protection (Data Protection Act), restrictions on the processing of personal data, the general prohibition on automated decision-making and provisions allowing

for data protection by design are vital in the regulation of AI systems. The level of protection given to AI technologies under the Consumer Protection Act is uncertain as it does not define goods. Therefore, it is unclear whether software would constitute 'goods' for the purposes of the Act. However, ICT/E-legislation and a consideration of intellectual property legislation, jurisprudence and soft law may be essential in ensuring that these technologies are utilised properly.