SOUTH AFRICA

DRAFT

ACRONYMS

ADM	Automated decision-making
AI	Artificial intelligence
BCR	Binding corporate rules
BSDC	Base Spatial Dataset Coordinator
DCDT	Department of Communications and Digital Technologies
DPHSR	Division of Public Health Surveillance and Response
DTA	Data transfer agreement
EOC	Emergency Operations Centre
FAIR	Findable, Accessible, Interoperable and Re-usable
GDPR	General Data Protection Regulation (Europe)
GIS	Geographical information system
HPCSA	Health Profession Council of South Africa
ICT	Information and communication technology
IP	Intellectual property
ITU	International Telecommunication Union
HREC	Human Research Ethics Committee
IHR	International health regulations
MRC	Medical Research Council
MTA	Material transfer agreement
NHA	National Health Act
NICD	National Institute for Communicable Diseases
NIPMO	National Intellectual Property Management Office
NSI	National System of Innovation
ORU	Outbreak Response Unit
PAIA	Promotion of Access to Information Act
PC4IR	Presidential Commission on the Fourth Industrial Revolution
PI	Principal investigator
POPIA	Protection of Personal Information Act
R&D	Research and development
SAHPRA	South African Health Products Regulatory Authority
SASDI	South African Spatial Data Infrastructure
SDIA	Spatial Data Infrastructure Act

DRAFT

Stats SA	Statistics South Africa
WHO	World Health Organization

DRAFT

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 Protection of Personal Information Act (POPIA) provides guidance on the use of informed consent. When undertaking genomic research, it is important to comply with the nature of informed consent required by POPIA.

Deciding if POPIA Applies

General health research allows for different forms of consent – for example, narrow consent and broad consent, according to ethical guidelines published by the Medical Research Council (MRC). However, under POPIA, consent applies only to health research involving the collection and processing of personal information in South Africa and its transfer abroad. In this regard, researchers, including genomic researchers, must seek specific informed consent from the data subject before dealing further with the data.

Exemptions/Scenarios when Consent is not Required

The *Government Gazette* should be checked for exemptions that may have been granted by the Regulator.

The need for consent may not apply if it is in public interest or if compliance is impossible or involves disproportionate effort. However, there should not be a disproportionately adverse breach of the privacy rights of the data subject.

Further Developments *after* Consent has been Given

- The data subject can withdraw consent at any time, without affecting the lawfulness of data processing *before* this withdrawal.

- When transferring data outside of South Africa, *further* specific consent is required from the data subject.

DRAFT

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 Pertinent Legal and Regulatory Framework

Many rights relevant to human genomics research are protected. These include the right to freedom of expression – and the right to freedom of scientific research and certain rights to engage in culture. These rights are established in the Constitution, but are also implemented in laws, regulations and guidelines. Several institutions regulate and support compliance in relation to human genomic research. These are the:

- Department of Health
- Department of Science and Technology
- Information Regulator
- National Health Research Ethics Committee
- Public Health Institute of South Africa
- South African Clinical Research Association
- South African Medical Research Council
- Technology Innovation Agency.

Individual Benefit Sharing

The approach to benefit sharing is:

(a) For research on human participants, the participant must be informed about: the expected and potential benefits of the research during and after the research; any incentives for participation; and beneficial products or interventions when the research is complete.

DRAFT

(b) According to the MTA for human biological materials, benefit sharing is defined very broadly and may include:

- Acknowledgement of the provider as the source of materials
- Capacity building
- Publication rights
- Royalties
- The sharing of information
- The use of research results
- The transfer of technology or materials.

Community Benefit Sharing

As researchers must consult with representatives from the participating community or other relevant research stakeholders, benefits may *transcend from individual to community benefits* and the parties must agree on how these will be shared.

That benefits may extend to communities or groups separate from individuals is affirmed by the recognition in South African law of research with 'collectives' – a term used to distinguish some distinct groups from informal communities and commercial or social groups. When conducting research with collectives, a researcher must ensure, among other things, that fair distribution of research-related benefits and harms among affected collaborating parties occurs. An agreement about ownership of data and the rights of publication of research findings must be put in place, together with an agreement about feedback to the collective about the findings.

Benefits

(a) Tissue donation and removal (and associated payment issues)

If any tissue, organ, blood or gametes are removed from any person, that person must give written consent, and where organs, blood, blood products, cultured cells, stem cells, embryos, foetal tissue, zygotes and gametes are to be exported from South Africa, the Minister for Health must approve this.

DRAFT

Furthermore, organs, blood, blood products, cultured cells, stem cells, embryos, foetal tissue, zygotes and gametes cannot be sold in South Africa. The donor cannot receive payment for such donations. However, the donor may receive compensation for costs incurred in making the donation. A person also cannot be paid for donating his/her human biological *data*.

A hospital or an authorised institution may, however, be paid for tissue or gamete acquisition, supply, importation or export, but there are limitations on the amount and purpose for which payment can be made. The payment must not exceed an amount which is reasonably required to cover the *costs* involved in the importation, export, acquisition or supply of the tissue, gamete, blood or blood product.

In terms of purpose, payment may be made only for:

- Health research and advancement of the health sciences
- Production of a therapeutic, diagnostic or prophylactic substance
- Therapeutic purposes, including the use of tissue in any living person
- Training of students in the health sciences.

(b) Patenting

Patenting is generally allowed, but several inventions cannot be patented, including inventions which would be expected to encourage offensive or immoral behaviour. Any variety of animal or plant or any biological process for the production of animals or plants, not being a micro-biological process or the product of such a process, also cannot be patented. The law does not mention patents relating to human genetic material.

DRAFT

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.

Legal clarity is provided on the use of people's geospatial data for public health surveillance. The privacy risks brought about by novel geospatial technologies are analysed and legal clarity is provided on how to comply with the relevant laws. The geospatial legal framework, the role of the Protection of Personal Information Act and other strategies, legal precepts and regulations are discussed.

Geospatial Legal Framework

Geospatial data or information about the location and names of features beneath, on or above the surface of the earth, is often obtained via near earth objects such as satellites. Therefore, consideration must also be given to the legislation that governs the use, access to and sharing of data generated or collected by these technologies in space.

Space Affairs Act, Spatial Data Infrastructure Act and the South African Spatial Data Infrastructure

The Space Affairs Act establishes a governing body for this purpose and provides for the establishment of a Council to manage and control certain space affairs in South Africa. The Spatial Data Infrastructure Act (SDIA) established the South African Spatial Data Infrastructure (SASDI) and the Committee for Spatial Information which is responsible for the management and monitoring of the activities of the SASDI and, most importantly, the data it generates – which is governed by the SDIA. This Act, which was developed to be implemented by organs of the state with active participation from the private geospatial information community, promotes the efficient and effective use of state resources across the different spheres of government, to cost-effectively centralise large volumes of spatial data to be readily available in an integrated format. The SASDI allows access to diverse geospatial

resources, integrating data from multiple sources via a reliable support environment, based on an established set of standards and formats to ensure optimum practical benefits to users.

The SDIA, together with the South African Geospatial Strategy, aims to provide strategic guidance to organs of the government to help them define the roles and responsibilities of the roleplayers in the implementation of the SDIA; to provide strategic direction to Stats SA (the Base Spatial Dataset Coordinator (BSDC)) in the implementation of the SDIA; and to provide a firm basis for the private sector and other stakeholders in the geospatial industry to develop their strategic business plans for contracting to government and for developing value-added products and services.

Base Data Set Custodian Policy

The Base Data Set Custodian Policy bases its access principles on the Constitution, which provides that everyone has the right of access to any information held by the state and any information that is held by another person which is required for the exercise or protection of any rights. The regulation of access and sharing of spatial information is the core of this policy, which states that access is a fundamental issue in the exchange of data. It further provides that spatial data must be *accessible to the public*. A data custodian is an organ of state or an independent contractor or person engaged in the exercise of a public power or performance of a public function, which captures, maintains, manages, integrates, distributes or uses spatial information, while a base data set consists of those themes of spatial information which have been captured or collected by a data custodian. All the spatial information themes and data custodians must disclose or make their thematic base data sets available to the public on request – unless exempted from disclosure under the Promotion of Access to Information Act (PAIA).

Pricing of the Base Data Set Custodian Policy

The Base Data Set Custodian Policy determines that base data set custodians must adhere to *standards* prescribed by the Minister in terms of the SDIA, and to any other relevant national standards for spatial information. However, because the infrastructure to enable the collection and sharing of spatial data may be expensive, data set custodians can charge for spatial information or base data sets in accordance with the Policy on Pricing of Spatial Information Products and Services. This pricing policy differentiates two distinct categories of spatial information products and/or services provided by public sector organisations: 1) products that are generally available from the organisation and are usually listed in its manual of records and

prepared in terms of PAIA; and 2) products and services that the organisation customises for the client on specific request (value-added products and services).

Principles of the South African Geospatial Strategy

To further fast track the implementation of the SASDI, the South African Geospatial Strategy proposes the adoption of five key principles:

1. Data must be collected once only and it must be kept where it can be maintained most effectively.
2. Seamless spatial information is to be combined from different sources across South Africa and shared with many users and applications.
3. Information must be collected at one level/scale and shared with all levels/scales and it must be detailed enough for thorough investigations and for strategic purposes.
4. Geospatial information needed for good governance at all levels must be readily and transparently available.
5. It should be easy to find what geospatial information is available, how it can be used to meet a particular need, and under which conditions it can be acquired and used.

South African Geospatial Strategy value chain

To understand geospatial information production, this strategy also proposes the adoption of a value chain for the entire process of collection, processing, analysis, maintenance and use of spatial information. The outcome of this value chain is to produce spatial data, products and services which will represent natural phenomena that include spatial information on rivers, mountains and natural vegetation; man-made phenomena that include spatial information on provincial and municipal boundaries; cadastre (land parcels and ownership); *addresses, place names and dwelling structures*; economic infrastructure phenomena that include spatial information on transport (road, rail and ports); water distribution and energy generation; and social infrastructure phenomena that include spatial information on housing, *health*, education, and municipal services. This spatial data can then be used as evidence in policy and programme development, spatial planning, monitoring and evaluation and decision-making.

Personal information and POPIA

DRAFT

In terms of data or informational privacy in the healthcare context, spatial data may be able to pinpoint the exact address, place names or dwelling structures of any individual. Although this information may be valuable when tracking and tracing people suffering from highly infectious and deadly or (yet) untreatable infectious diseases, there is also the individual's constitutional right to privacy to consider and the balance with the public's right to health and a healthy environment.

POPIA governs the *processing of personal information by the public and private sectors*. In this context, the responsible party who is allowed to process personal information, subject to certain conditions contained in POPIA, means any other person, from a public or private body, who, alone or with others, determines the purpose of and means for the processing of personal information. This definition includes the organs of the South African government that define the roles and responsibilities of the respective role players in the implementation of the SDIA. If such an organ of state processes *personal information* of an individual, POPIA is applicable.

Personal information in relation to geospatial data in the context of POPIA

Personal information is defined in POPIA as information relating to an *identifiable, living, natural person.* It includes information relating to such a person's race; national, ethnic or social origin; colour; sexual orientation; age; physical or mental health; disability; religion; beliefs; culture; language; and information relating to any identifying number, symbol, *physical address, location information*, online identifier or the name of the person if it appears with other personal information relating to the person. Such information may enable identification of an individual based on his or her physical location or geolocation. It can also provide a good indication of such a person's national, ethnic or social origin depending on that person's geolocation. Accordingly, geospatial data is personal information.

In biomedical research, certain communities or areas are frequently targeted for specific types of research. If geospatial information about these communities is then combined with medical records or clinic visits and the health status of members of that community, a specific individual can be identified.

Geospatial information and special personal information in the context of POPIA

Although POPIA further distinguishes between personal information and special personal information, it is doubtful that geospatial information can be considered to be special personal information, because it is not listed, defined or referred to in the definition of special personal information. Special personal information is defined as religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life or biometric information of a data subject, or the criminal behavior of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence. *However*, considering the physical harm that may befall an individual whose physical location has been disclosed, geospatial information or the combination of geospatial information with other identifying information could probably receive the additional privacy or informational protection reserved for special personal information. The legal and ethical challenges posed by immigration surveillance are an example of the challenging scenarios that the combination of geospatial data, surveillance, privacy, and national security can produce.

POPIA applies only to personal information and *not* to any information disclosing the whereabouts of groups of people, communities, populations, or any other collective of persons.

Conditions when POPIA does not apply to the processing of personal information

POPIA also does not apply to any processing of personal information if such information has been:

- de-identified to the extent that it cannot be re-identified again;
- processed by or on behalf of a public body which involves national security, including activities aimed at assisting in the identification of the financing of terrorist and related activities, defence, or public safety;
- processed for prevention and detection, including assistance in the identification of the proceeds of unlawful activities and the combatting of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information;
- processed by the Cabinet and its committees or the Executive Council of a province; and
- processed in relation to the judicial functions of a court.

DRAFT

Therefore, any information that can be used for the national defence of the country, national security, crime prevention or law enforcement falls outside the ambit of POPIA, meaning that organs of state in these circumstances are exempted from obtaining consent for using individuals' personal information, which may include their geospatial information. Geospatial information as set out in the SDIA may be valuable when defending the country or tracking criminals for terrorist and related activities.

POPIA, personal information, and consent to data processing

POPIA determines that personal information may be processed only if the data subject (or a competent person where the data subject is a child) consents to the processing. Considering that a person may not always be aware that his or her physical address or location information are being processed as the technologies used to process such data are often far removed from the person, the data subject must be notified when his or her personal information is being collected. This places the burden on the data processor to ensure that the data subject is aware of the data processing. POPIA further requires data processors to show the reasonable steps they took to bring this specific processing to the attention of the data subject – before information is collected or as soon as is reasonably practicable.

Circumstances when data processors are exempt from notifying individuals about data collection

- If the data subject or a competent person (where the data subject is a child) has provided consent for the non-compliance;
- Where non-compliance would not prejudice the legitimate interests of the data subject as set out in POPIA;
- Where non-compliance is needed to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
- To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in the South African Revenue Service Act;
- For the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated;
- In the interests of national security;
- Where compliance would prejudice a lawful purpose of the collection;

- Where compliance is not reasonably practicable;
- Where the information will not be used in a form where the data subject may be identified; and
- Where the data is used for historical, statistical or research purposes.

South African Digital Health Strategy and its key principles

The South African Digital Health Strategy is underpinned by five key principles, which include innovation for sustainable digital health impact. It envisions a change to the way things are being done by adding technologies and transforming the way people interact with their own health decisions and receiving or providing care in the healthcare system. A key intervention in this regard is the establishment of a data science capability to source technologies such as big data, artificial intelligence and predictive analytics for enhanced benefits of the digital health ecosystem – especially more sustainable health system approaches and evidence-based clinical decisions. Although this strategy supports the integration of data-generating technologies to inform healthcare, it does not mention or provide for the use of the integration of geospatial data into the healthcare system. Instead, the strategy takes an individualistic and focused approach. However, a broader view must be considered where geospatial data and its value in the prediction of natural disasters or the spread of infectious diseases must be considered and how it can be applied to more effectively to manage health emergencies.

National Strategies and the Presidential Commission

National Digital and Future Skills Strategy

This Strategy recognises the service industries, including health services, as being in the process of being transformed by digital automation, artificial intelligence (AI) and a range of other digital technologies. Technologies that enable the collection, interpretation and sharing of geospatial data must be exploited for their value to the delivery of public healthcare management and related services.

Presidential Commission advising government on the Fourth Industrial Revolution

Infrastructure, resources and the natural environment are some of the key focus areas of the Presidential Commission advising government on the Fourth Industrial Revolution. This focus, together with the aims of the South African Geospatial Strategy, could lead to significant developments in the successful implementation and use of geospatial technologies and infrastructure.

World Health Assembly and the International Health Regulations

Internationally, there is increasing pressure from the World Health Assembly that member states adhere to the International Health Regulations (IHR). Signatory countries have been requested to host a Joint External Evaluation of adherence to requirements of the IHR, which include activities to support prevention, detection and response to communicable disease, and chemical and radiation events. The contribution of the National Institute for Communicable Diseases (NICD) includes capacity for communicable disease diagnostics, disease surveillance and technical support for response activities – and this supports many of the requirements of the IHR. The Emergency Operations Centre (EOC) supported by the Outbreak Response Unit (ORU) can provide coordination and management of public health events of national and regional concern through the use of an incident management system and dedicated staff. On account of these capacities, the NICD is a key role player in national, regional and international responses to public health threats. The Division of Public Health Surveillance and Response (DPHSR) collaborates and cooperates with the National Department of Health, the National Disaster Management Centre, and the National Joint Operations Committee in support of the IHR. Disease intelligence emanating from NICD surveillance activities is reported regularly through the Multinational Outbreak Response Team and other government structures.

Conclusion

South Africa already has a huge network of role players that use spatial information, but mainly in agriculture and land ownership. There are a limited number of private-sector role players that are using GIS technologies for healthcare purposes, which is evidence that these technologies can be applied with success for managing health emergencies brought about by natural disasters or infectious diseases. South Africa also recently issued various strategies for digital technology development, including the development of these technologies for the health sector. However, none of these technologies specifically provide for GIS technologies and

DRAFT

therefore the connection between data generated by GIS technologies and its value for the healthcare sector is still misunderstood and undervalued.

DRAFT

CROSS-BORDER SHARING OF DATA

This section reviews the rules as required by data protection law in the cross-border sharing of personal data. The rules on the cross-border sharing of personal data under data protection law do not exist in a vacuum, and therefore other important information that must be followed when sharing personal data is discussed. This information, however, is comprehensive as it relates to the cross-border sharing of personal data.

The relevant national health research regulations as they relate to the cross-border sharing of personal data are reviewed. These national health research regulations set out the required legal and ethical conditions that must be met when processing personal data for research. Applicable national legal and ethical documents are listed, but the discussion only specifies the requirements as they relate to the cross-border sharing of personal data for research. The guide does not treat the legal and ethical requirements generally required for research, and therefore users of this guide must consult with these documents to ascertain these requirements and to ensure that they are met.

An overview of the data protection law (POPIA) is provided. This includes what data POPIA applies to, the categories of data, the key individuals in POPIA, the key principles required to be met in the processing of personal data, and the rights of data subjects. This is an overview only to help users to understand *some* of the requirements of POPIA and to begin to assist users in navigating the Act. It is not comprehensive, and users of POPIA must consult it to understand all relevant and applicable requirements to be met, and to understand any exceptions that may be in place for research. This is necessary as all these requirements must be met in the processing of personal data for research, in addition to the requirements on cross-border sharing of data.

The section provides users with a comprehensive description of the requirements to be met in the cross-border sharing of personal data for research. It sets out all the necessary conditions that must be met to legally share data across borders for research.

In countries where no data protection law is in force, the necessary national legal and ethical requirements, as they relate to the cross-border sharing of data, are presented.

The cross-border sharing of personal information is governed by several laws and regulations, which must be carefully considered and complied with before researchers share data for research purposes. In South Africa, the Protection of Personal Information Act is a general data protection law that applies to the processing (i.e., use) of personal information in all sectors. While it is not a statute introduced specifically to regulate research, it applies to research that involves the processing of personal information. It is only one of several laws that must be complied with when transferring personal information for research purposes.

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

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

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

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

These laws, regulations and guidelines set out the legal and ethical requirements that must be met for the conduct of research in South Africa and must be considered when effecting cross-border data transfer of personal information. Furthermore, if health researchers seek to transfer any human biological material (along with its accompanying data), the National Material Transfer Agreement (SA MTA) requires that a relevant Human Research Ethics Committee (HREC) first approves the MTA before a transfer can occur.

Protection of Personal Information Act (POPIA)

In addition to these legal and ethical requirements, POPIA applies to the processing of all personal information, but in acknowledging the importance of research, special provisions are

in place that deal with the processing of information purely for research purposes. In addition, extra conditions must be met prior to the transfer of personal information across borders.

Some of the techno-legal terms used in POPIA are listed and discussed below. This is not a thorough assessment of the Act as it applies to research, but rather an overview of some of the key terms and conditions that must be met in the processing of personal information for research.

The Main Actors Defined in the Protection of Personal Information Act

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

Categories of Data Listed in the Protection of Personal Information Act

	Legal definition	Layman explanation
Personal information	Information relating to an identifiable, living, natural person, and where it is applicable, an	Information about a particular person that can identify him or her.

	identifiable, existing juristic person, including, but not limited to: (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.	
Special personal information	This is referred to in POPIA as follows: A responsible party may, subject to section 27, not process personal information concerning: the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject.	This is sensitive personal information about a particular person, such as health data and genetic data, and which receives additional legal protection.
De-identify	In relation to personal information of a data subject, this means to	To de-identify personal information, any information that can be used to

DRAFT

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

Information is considered to be personal when it relates to an identified or identifiable person. It is this personal information that data protection law seeks to protect. Data protection law does not concern or apply to de-identified non-personal information. De-identified data is explicitly excluded from POPIA. This is particularly useful for scientists who, by de-identifying their information, will not need to comply with data protection laws. De-identifying information is the process of stripping the data of any information which can be used to identify a data subject. It should not be possible to re-identify the data subject, directly or indirectly, by manipulating the information or linking it with other information.

It can be challenging to assess whether the information you intend to share is de-identified, especially in light of fast-paced technological advancements powered by artificial intelligence. While there is no guidance from the Regulator on this point, general principles are worth highlighting.

The GDPR, for instance, adopts a risk-based approach, considering factors such as the likelihood of re-identification, and considering cost, time, and technological advancements. POPIA, on the other hand, focuses on whether a *reasonably foreseeable* method exists that could re-identify a data subject. Unlike the GDPR, POPIA's test does not require that the method is *likely* to be *used*; it is enough that the method foreseeably *exists*.

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

DRAFT

On this, there are two possibilities:

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

The first test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to data Controller B, the dataset would not be de-identified non-personal information.

The second context-specific test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Data Controller B, the dataset *may* be considered de-identified non-personal information in the hands of Data Controller B. A test would be needed to determine whether the dataset is de-identified in the hands of Data Controller B.

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

- An assessment must be made on a case-by-case basis, considering the particular context.
- The de-identification must be irreversible.
- The assessment is made on the current state of the art. As technology progresses, information once deemed to be de-identified may become personal information and 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, such as whether a method of re-identification is *reasonably likely* to be used (considering, for example, technology, resources and time to identify the data subject) so that it is possible to take appropriate steps to guard against these risks. However, this is insufficient to comply with POPIA's test for de-identification. If a

DRAFT

reasonably foreseeable method *exists* that can be used to identify the data subject, no matter how unlikely it could be used, the information will remain personal information.

- It is possible to follow the GDPR test which states the data is anonymous if an individual cannot be singled out, or identifiers cannot be linked to make a person identifiable, or it is impossible to infer a link between two pieces of information in a dataset.
- Genetic data is considered to be special personal information. It not only falls under the data protection law but has a higher level of protection under POPIA.
- There is an ongoing debate about whether genomic datasets can ever be rendered truly de-identified, particularly as genetic data is an identifier. In considering whether a genomic dataset can be considered de-identified, context matters – i.e., consider the objective factors related to the information.

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

1. *Purpose specification*: Personal information should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that the purpose must be clearly set out. There are certain exceptions for research.
2. *Processing limitation*: Only the data that is necessary for the specific purpose should be collected and processed.
3. *Information quality*: Personal information must be accurate and, where necessary, kept up to date. Processes should be in place to ensure that all personal information collected is accurate.
4. *Further processing limitation*: The processing of personal information should be used only for the purpose for which it was collected, unless the purpose falls within one of the exceptions (for example, research).
5. *Openness*: The responsible party must maintain documentation of all processing activities and must inform the data subject about the processing of his/her personal information.
6. *Data subject participation*: This details the rights of the data subject. There are some exceptions for research.
7. *Security safeguards*: Personal information should be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing

DRAFT

and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Both organisational and technical measures must be put in place to secure the data.

8. *Accountability*: The responsible party is responsible for, and must be able to demonstrate compliance with, the principles mentioned above. It is good practice to keep a record of data processing activities, measures introduced to protect the data, and any risk assessments made. This can be used to demonstrate compliance in the event of a breach.

Data Subject Rights Under the Protection of Personal Information Act

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

1. *Right to be informed*: The data subject has the right to be informed about what his/her personal information will be used for. This right can be exempted if the personal information has not been collected directly from the data subject and the processing is for research.
2. *Right to access*: The data subject has the right to access personal information that the responsible party has about them. The responsible party should have a process in place to facilitate this.
3. *Right to rectification*: The data subject has the right to have inaccurate personal information corrected and incomplete data completed.
4. *Right to erasure*: The data subject has the right to request that his/her data be erased.
5. *Right to restriction of processing*: The data subject can request that the responsible party stop processing his/her personal information.
6. *Right to object*: The data subject can object to the processing of his/her personal information where the lawful basis of processing is not consent.
7. *Rights in relation to automated decision-making and profiling*: The data subject has the right to object to a decision based solely on automated processing information which is intended to provide a profile of the data subject.

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

Cross-Border Data Sharing

DRAFT

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

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

1. There must be an adequate level of protection in the form of a law, binding corporate rules (BCR) or a binding agreement (data transfer agreement (DTA)).
2. The data subject consents to the transfer.
3. The transfer is necessary for facilitating a contract between the data subject and the responsible party.
4. The transfer is necessary for a contract, in the interest of a data subject, between the responsible party and a third party.
5. The transfer is for the benefit of the data subject and not the general public.

DRAFT

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

No AI legislation has been promulgated in South Africa. 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

Several sector-specific policy documents speak to AI development and its use. These include the:

- Draft National Policy on Data and Cloud, 2021
- National Digital and Future Skills Strategy, 2020
- National Digital Health Strategy, 2019–2024
- National e-Strategy, 2017–2030
- Presidential Commission on the Fourth Industrial Revolution (PC4IR) Report
- White Paper on Science, Technology and Innovation, 2019.

These documents include AI in the definitions of 'digital industrial revolution' (National e-Strategy, 2017–2030), 'digital health' (National Digital Health Strategy, 2019–2024), and 'digital economy' (Draft National Policy on Data and Cloud, 2021).

White Paper on Science, Technology and Innovation, 2019

This identifies funding for scientific research as a national priority and acknowledges inclusion as vital to establishing a coherent national system of innovation. The strategy highlights that new institutional frameworks to manage convergence and increased R&D focused on enabling technologies will be required if the full promise of the 4IR is to be realised. While advancing

knowledge in new fields, these arrangements must promote university research in fields connected to current base technologies. A proposed high-level national collaborative platform – geared to help identify and support priority programmes linked to the 4IR and to contribute to the development of a South African strategy on AI – is intended to position South Africa to respond to the opportunities and risks arising from the 4IR. It will be managed by a steering committee that includes relevant departments and business and labour, in a bid to focus on strategies to address potential job losses in affected industries. A South African AI Strategy will be able to capture the country's involvement and contribution to the development of AI knowledge, technology, and applications in the context of bolstering the National System of Innovation (NSI) and helping mitigate the potential negative effects of AI.

National Digital Health Strategy, 2019–2024

This includes AI in the definition of digital health and identifies innovation as a core aspect. It is underpinned by five key principles, including innovation for sustainable digital health impact. Digital health is viewed as a mechanism for transforming the way we interact with our own health decisions and receiving or providing care in the healthcare system through increased automation, the use of emerging technologies such as AI, and the introduction of greater efficiencies. Under the strategic component, services and applications, a key intervention is to establish a data science capability for sourcing emerging technologies such as AI to ensure beneficial and sustainable health systems and to allow for evidence-based clinical decision-making.

None of the above policy documents supersede one another. However, the most significant contributions to AI regulation are the PC4IR Report and the Draft National Policy on Data and Cloud, 2021.

The Presidential Commission on the Fourth Industrial Revolution

The PC4IR has been tasked with proposing the country's overarching strategy for the 4IR and recommending the institutional frameworks and roles of the various sectors of society within the broad plan. There are eight key lessons and dimensions of strategy for South Africa: service delivery; the central role of state; regulations and ethics; preparation through experimentation; private sector capabilities; human capital development; technological clarity and commitment; and global leadership.

DRAFT

Within the Commission, an emerging set of principles will guide the development of policy and legal recommendations: policy must be inclusive; duplication and fragmentation of infrastructure development must be avoided; policy must incentivise entrepreneurs; policy must be adaptive; and social economic impact assessment system consultation and extensive stakeholder consultation are vital.

Key recommendations of the Commission include: (1) investment in human capital; (2) establishing an AI institute; (3) establishing a platform for advanced manufacturing and new materials; (4) securing and availing data to enable innovation; (5) incentivising future industries, platforms and applications of 4IR technologies; (6) building 4IR infrastructure; (7) reviewing and amending (or creating) policy and legislation; and (8) establishing a 4IR Strategy Implementation Coordination Council in the Presidency.

Three key health-sector initiatives that AI and other emerging technologies are intended to drive are: the use of telemedicine; the coordination and interoperability of health information systems; and the development of a digital supply chain using predictive analytics.

The Draft National Policy on Data and Cloud, 2021

This Draft National Policy is a means to empower the AI Strategy to be pursued in the PC4IR's proposed AI Institute. The AI Institute is understood to be a facility for training, R&D, and is intended to advance the use of AI for resolving challenges that South Africa faces. The Commission also recommends an ICT infrastructure framework that will support key economic sectors for digital development. Such infrastructure should address not only the need for storing and accessing data, but also the need for the computing power that is necessary to process data.

The Draft Policy suggests several relevant policy interventions, including: the Minister establishing an Advisory Council to advise on the development of an AI code of ethics, among other things; and the Department of Communications and Digital Technologies (DCDT) establishing an institutional mechanism aimed at studying the impact of 4IR technologies, for example, the AI Institute.

Data is a key component/asset in the application of AI and must thus comply with the FAIR principles: it must be Findable, Accessible, Interoperable and Re-usable.

Digital Health/e-Health

AI falls under digital health which derives its guidance from the standalone National Digital Health Strategy for South Africa 2019–2024. No legislation addresses predictive software/AI as a medical device in South Africa. Nonetheless, medical devices in South Africa are regulated by the South African Health Products Regulatory Authority (SAHPRA) as stipulated in the Medicines and Related Substances Control Act. Therefore, SAHPRA will be the regulatory authority of AI use in healthcare. The digital health strategy was developed by adapting the WHO/International Telecommunication Union (ITU) National eHealth Strategy Toolkit and building on the previous e-Health developments and interventions. The Minister of Health is on the regulatory board for digital health and is advised by the National Health Council as mandated by the National Health Act.

Telemedicine

No standalone legislation regulates telemedicine. However, the Health Profession Council of South Africa (HPCSA) general ethics guidelines provide for e-Health or telemedicine codes of practice.

The HPCSA regulates the professional medical conduct of all healthcare practitioners in South Africa. Medical practitioners in South Africa are defined by law and are required to be registered in terms of the health professions and the National Health Act. Medical research in South Africa is regulated by the National Institute for Medical Research Act, which would inadvertently cover AI use in health research.

Consumer Protection & ICT/E-Legislation

Statute	Consumer Protection Act
Strict liability	Producer; importer; distributor; retailer
Software as goods	Yes
Electronic consumer protection	Electronic Communications and Transactions Act
Cybersecurity	Cybercrimes Act

DRAFT

No content control measures exist in South African law. However, the following are criminal offences under the Cybercrimes Act: hacking (unlawful access to data, unlawful interception of data and unlawful interference with data or computer systems, including use of malware); possession or use of software or other tools intended to be used for hacking; unlawful acquisition of or use of passwords or access codes; cyber fraud; cyber forgery; cyber extortion; and malicious communications.

Data Protection Law

While no AI legislation has been developed, data protection law will heavily influence the uptake of AI systems in the country. Relevant provisions of the Protection of Personal Information Act (POPIA) include: rights to opt-out/opt-in; notice and consent requirements; minimum standards of data protection; and restrictions on offshore data transfers. Particularly important are restrictions on the processing of sensitive data, authorisation for the processing of personal information, and the general prohibition on automated decision-making.

Prohibition on the processing of special personal information

There is a general prohibition on the processing of special personal information. Grounds when this does not apply, include when: consent is obtained; the processing of personal information is necessary for a right or obligation in law; processing is for historical, statistical or research purposes; or if information has deliberately been made publicly available by the data subject.

Conditions for processing of personal health or sex-life information

Processing of personal information concerning a data subject's health or sex life may occur when processing is necessary for:

- the proper treatment and care of the data subject;
- institutional administration or professional practice;
- insurance purposes including assessment of risk, performance or enforcement of rights and obligations;
- providing special support for pupils;
- any public or private body to manage the care of a child;

DRAFT

- any public body to implement prison sentences or detention measures; and administrative bodies or institutions to implement the provisions of law or reintegration of or support for those entitled to benefit in relation to sickness or work incapacity.

In the above instances, responsible parties may only process information subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject. A duty of confidentiality is placed on the responsible party permitted to process information, where there is no obligation of confidentiality.

Processing of personal information concerning inherited characteristics of a data subject

This processing is prohibited, unless a serious medical interest prevails or processing is necessary for historical, statistical or research activity.

Prohibition on automated decision-making and list of exemptions

Solely automated decisions which result in legal consequences, or which affect the data subject to a substantial degree, are prohibited. Exemptions from the prohibition on automated decision-making (ADM) include: instances in which the resultant decision has been taken in light of a contract for which the requests of the data subject have been met or the data subject's legitimate interests are protected by appropriate measures. Further instruction on the appropriate measures to be taken by the responsible party should provide an opportunity for a data subject to make representations in relation to a given decision. The responsible party is required to provide sufficient information about the underlying logic of the automated processing to enable the data subject to make such representations. The general prohibition on ADM does not apply where the legitimate interests of the data subject are protected by a law or code of conduct specifying appropriate measures.

Guidance notes provided by Office of the Information Regulator

These notes relate to: (1) prior authorisation applications; (2) Information Officers and Deputy Information Officers; (3) exemptions from the requirements for lawful processing; (4) the processing of personal information of children; and (5) the processing of special personal information.

Intellectual Property

The South African intellectual property environment is mature, and is governed by various legislative provisions, jurisprudence and soft laws. The legislation is the:

- Intellectual Property Rights from Publicly Financed Research and Development Act
- South African Copyright Act
- South African Patents Act.

The common law governs trade secrets. The soft law includes the:

- Draft IP Policy 2018 Phase 1
- Draft National Open Science Policy 2022
- National Intellectual Property Management Office (NIPMO) guidance note
- Presidential Commission on the Fourth Industrial Revolution, 2020
- Proposed National Data and Cloud Policy, 2021
- White Paper on Science and Technology, 1996
- White Paper on Science, Technology and Innovation, 2019.

Summary and Analysis

While several policy documents on AI development and use have been produced, relevant provisions in promulgated legislation will take precedence over other regulatory/policy documents. These policy documents are interoperable and do not supersede one another. They highlight similar challenges and solutions such as the need for inclusion and infrastructure development. These instruments work together to create a broader framework for AI development and use, geared towards developing a South African AI Strategy. New regulatory developments such as the PC4IR Report and Draft National Data and Cloud Policy are vital in ensuring that practicable steps are being taken to encourage the development and use of AI-based technologies.

Regarding digital health, medical devices – regulated by SAHPRA – are subject to the Medicines and Related Substances Control Act. Other important legal instruments include the Health Professions Act, National Health Act, South African Medical Research Council Act, as

well as the HPCSA general ethics guidelines which allow for telemedicine/e-Health codes of practice.

Within the legal framework for data protection, restrictions on the processing of personal data and the prohibition on automated decision-making are vital in the regulation of AI systems. AI technologies may receive some protection under the Consumer Protection Act as software is included in the provided definition of 'goods'. Furthermore, ICT/E-legislation such as the Electronic Communications and Transactions Act and Cybercrimes Act and a consideration of intellectual property legislation, jurisprudence and soft law may be important for ensuring that these technologies are used properly.

DRAFT