RWANDA

ACRONYMS

AI	Artificial intelligence
CGIS	Centre for Geographic Information Systems and Remote Sensing
CSP	Communication service provider
DPP	(Personal) Data Protection and Privacy
DRM	Disaster risk management
GIS	Geographic information system
ICT	Information and communication technology
IP	Internet protocol
ISR	Intelligence, surveillance and reconnaissance
NSDI	National Spatial Data Infrastructure
PI	Principal investigator
RBC	Rwanda Biomedical Centre
RSA	Rwanda Space Agency
RURA	Rwanda Utilities Regulatory Authority
UAS	Unmanned Aircraft System
UNESCO	United Nations Educational, Scientific and Cultural Organization

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 data protection legislation is the Law Relating to the Protection of Personal Data and Privacy (DPP Law) (2021).

Law Relating to the Protection of Personal Data and Privacy

In this legislation, genetic information is classified as sensitive personal data. The legislation imposes a general obligation on the data controller, data processor or a third party to not infringe the privacy of the data subject. There is no research exemption provision.

Consent to the processing of personal data

The data subject must consent to the processing of personal data for a specified purpose. The consent must be made freely after being informed of the consequences of consent.

Consent to the processing of sensitive personal data

One of the grounds for processing sensitive personal data, which includes genetic information, is that the processing is based on the data subject's consent. The data subject can also consent to the collection of his or her personal data from another source.

Withdrawal of consent

The data subject can withdraw consent at any time, but this does not affect the lawfulness of processing of personal data based on consent before the withdrawal. After the data subject withdraws consent this will take effect from the date on which the data subject applied for it.

Consent and sharing/transferring personal data outside of Rwanda

Consent of the data subject is required when this action takes place.

INDIVIDUAL AND COMMUNITY RIGHTS IN GENOMIC DATA

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

Many rights relevant to human genomics research are protected. These include the right to life; inviolability of the human being; right to physical and mental integrity, including the right not to be subjected to experimentation without consent; and the right to participate in activities that promote national culture. These rights are provided for in the Constitution and are implemented in legislation, regulations and policy guidelines.

Regulatory and Supporting Institutions

A number of institutions are involved in regulating and supporting compliance with human genomic research. These are the:

- Ministry of Health
- Ministry of ICT and Innovation
- National Industrial Research and Development Agency
- Rwanda Biomedical Centre
- Rwanda Forensic Laboratory
- Rwanda Information Society Authority
- Rwanda National Commission for UNESCO
- Rwanda National Ethics Committee
- Rwanda National Health Research Registry
- Rwanda Utilities Regulatory Authority

Individual and Community Benefit Sharing

Although not yet signed into law, the Draft Law Relating to Research on a Human Participant proposes that research carried out in Rwanda should promote the transfer of technology for the benefit of the national institutions that have participated in research, and that research participants should benefit from research. Researchers must publish and disseminate their findings in a manner that aims to maximise the study's benefits and impact and which also ensures that resources that are directed to research improve the health sector.

Benefits

(1) Tissue donation, removal and associated payment

For any tissue, organ, blood or gametes to be removed from any person for purposes of treatment, that person must give written consent. However, consent may not be required in emergencies. Human body organs and products used in treatment cannot be sold. Payment cannot be made to anyone who offers his/her body for experimentation, or one who donates his organs or products of his/her body to be used for therapeutic purposes.

Human body organs and products must not be used for therapeutic purposes if their negative effects exceed expected advantages for the recipient and no human product should be used from persons with transmissible diseases that can affect the donor's or the recipient's health. The purpose of donation and removal of human organs, tissue, blood or gametes is limited to therapeutic, educational and scientific use of organs and human body products.

(2) Patenting

Patenting of new inventions is allowed and encouraged. Even though the law does not mention patents relating to human genetic material, the following inventions are excluded from patenting:

- Discoveries, scientific theories and mathematical methods

- Schemes, rules or methods for doing business, and performing purely mental acts or playing games
- Methods for treatment of the human or animal body by surgery or therapy, and diagnostic methods practised on the human or animal body
- Substances – even if purified – synthesised or otherwise isolated from nature
- Known substances for which a new use has been discovered
- Plants and animals, including their parts, other than microorganisms and biological processes for the production of plants or animals and their parts, and other than non-biological and microbiological processes and products obtained from those processes
- Animal and plant varieties
- Pharmaceutical products for international conventions to which Rwanda is a party
- Inventions whose commercial use is contrary to public order and morality.

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.

In terms of the legal framework, the relevant legislation, draft legislation, guidelines and policies are discussed below.

Rwanda's data protection statute does not have laws regulating geospatial data.

General Framework

(a) Legislation

The Rwandan Constitution

As geospatial data affects privacy when it identifies individuals, data controllers must give careful consideration to general privacy protections applying under Rwandan constitutional law.

The confidentiality of correspondence and communications is protected under the Constitution except in circumstances and in accordance with procedures determined by the law. Furthermore, Rwanda has ratified the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which protects the right to privacy. In addition, there is the Resolution on Democracy in the Digital Era and the Threat to Privacy and Individual Freedoms. Rwanda is committed to, among other things, ensuring that all legislation in the field of surveillance, privacy and personal data is based on the principles of legitimacy, legality, transparency, proportionality, necessity, and the rule of law. Lastly, during Rwanda's 3rd Universal Periodic Review, it accepted 14 out of 53 recommendations it received related to the right to freedom of expression – committing to strengthen its legal system and revise provisions

that undermine this right. These recommendations are integral to ensuring the fulfilment of the above legal obligations.

Law No 058/2021 relating to the Protection of Personal Data and Privacy (DPP Law)

The Data Protection Law (DPP Law) sets out a comprehensive framework for the protection of personal data. One of the tenets of the DPP Law is the clear and unambiguous consent of an individual to the collection, storage, and processing of personal data, which is a fundamental right. Prior to this law, other legal provisions provided for data and privacy protection and these were scattered across different laws, including the Constitution which guarantees protection of privacy for persons and family as a fundamental right.

All organisations that collect or process personal data in Rwanda must take steps to ensure that they are compliant with the law.

The DPP Law contains no definition for health data but defines personal data as any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person. The DPP Law will apply to the processing of geospatial data, such as location information, where it renders an individual identifiable.

The DPP Law further distinguishes between personal information and sensitive personal information. It defines sensitive personal data as information revealing a person's race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life, or family details.

Rwanda does not have laws specifically regulating geospatial data. However, as geospatial data has privacy impacts where it identifies individuals, it is necessary for data controllers to give careful consideration to the general privacy protections applying under Rwandan constitutional law.

These considerations merit special attention by health researchers combining geospatial data with health data, medical records and genetic or biometric information, in such a way that individuals may be identifiable. However, outside of these special cases it is doubtful that geospatial information can be considered to be sensitive personal information because it is not listed, defined, or referred to in the definition of sensitive personal information.

The DPP Law sets out a comprehensive set of principles for the lawful processing of personal data. The penalties for non-compliance can be severe. It provides for an administrative fine of up to 1% of the global turnover of the preceding financial year for corporate bodies and legal entities.

Rwanda drone laws

Rwanda's drone laws may also affect the collection of geospatial data and/or the surveillance and consequent identification of persons. The Rwanda Civil Aviation Authority has issued Regulations related to Unmanned Aircraft System (UAS) operation and an Advisory Circular RCAA-AC-UAS-21-001, which should be consulted.

ITC/E-legislation

Reference should be made to both the Law No 60/2018 on Prevention and Punishment of Cyber Crimes and Law No 24/2016 Governing Information and Communication Technologies that apply to governance of the electronic sphere in Rwanda. The purpose of the Law on Prevention and Punishment of Cyber Crimes is to prevent and punish cybercrimes that are committed in Rwanda or committed outside of Rwanda but which have an effect in Rwanda. The Law Governing Information and Communication Technologies applies to the broadcasting sector, information society, and electronic communications and some of the purposes of this Law are to promote the use of information in such a manner that the quality of both life and work are improved, and also to establish Rwanda as a global hub for multimedia information.

(b) Ancillary legislation

Law 30/2013 relating to the Code of Criminal Procedure

Under this Law, if all other investigative procedures for uncovering evidence to establish the truth in relation to an offence against national security have been unsuccessful, then the public security organs may, upon written authorisation from a competent National Prosecutor appointed by the Minister in charge of justice (the Prosecutor General of Rwanda or his delegates) intercept private communications, including communications made by telephone, email, over the internet, or by other means. Such authorisation must be in writing, containing details of "items or connections" to be intercepted and indicating the relevant offence being investigated. If required by "urgent public security interests", the interception warrant can be verbally issued by the National Prosecutor, but this must be followed by a written warrant within 24 hours, otherwise the interception will be presumed illegal. Authorisation of interceptions under this law are valid for three months but can be renewed for another three-month period. A person whose communications are unlawfully intercepted may file a complaint with the High Court (or the Military High Court for those in the military). However, the filing of such a complaint does not entail suspension of interception.

Law 60/2013 regulating the Interception of Communications

This Law reaffirms and extends the provisions under Law 30/2013 relating to interception of communications. It states that the interception of any communication made by means of a public or private communication system without authorisation from a competent authority is unlawful and that a warrant for lawful interception can be granted by a National Prosecutor designated by the Minister in charge of justice. Only specified security organs are authorised to apply for such a warrant. If required by "urgent public security interests", the interception warrant can be verbally issued by the National Prosecutor, but this must be followed by a written warrant within 24 hours, otherwise the interception will be presumed illegal. Communication service providers (CSPs) must ensure that their systems are technically capable of supporting interceptions at all times. All entities authorised to carry out lawful interception must be notified of any upgrade to an electronic communications network or service. However, any competent security organ making an application for an interception warrant may request a warrant to intercept the communications directly, without recourse to a communication service provider. In practice, this is conducted by the National Intelligence and Security Service of Rwanda as the entity entitled to possess the necessary equipment for such direct interception under the Law

Relating to Arms 33/2009. The Law provides for inspectors to be appointed by Presidential Order to monitor authorised persons and ensure that they intercept communications in accordance with the law. This role is performed by a police officer if requested by the Criminal Investigation Department or the National Intelligence and Security Service and if requested by the Prosecutor General's Office. This law strictly prohibits the interception of communications of the Rwandan President.

Law 24/2016 governing Information and Communication Technologies

In order to protect the public from any threat to public safety, public health or in the interest of national security, the Minister in charge of ICT can direct the Rwanda Utilities Regulatory Authority (RURA) to suspend or restrict a legal or natural person's entitlement to provide an electronic communications network or service or any associated facility. This enables the government to require CSPs to shut down their networks in such situations. Any aggrieved party can appeal such a decision to RURA and a further appeal can be made to a competent court.

According to the Law, no person may send a message or any other matter that is grossly offensive or is of an indecent, obscene, or menacing character by means of a public electronic communications network or cause such a message or matter to be sent. It also states that no person may send or cause to be sent false messages by means of a public electronic communications network or persistently use a public electronic communications network to cause annoyance, inconvenience or needless anxiety.

In matters related to national sovereignty and in a bid to comply with national legislation and international instruments ratified by the country, the Law gives the Minister in charge of ICT the power to:

- interrupt or cause to be interrupted any private communication that appears to be detrimental to national sovereignty, or contrary to any existing law, public order or good morals;
- suspend, wholly or in part, any electronic communications service or network operations for a specified or undetermined period; and/or
- requisition or cause to be requisitioned any electronic communications infrastructure.

These powers may be used by the Minister in charge of ICT to require that CSPs block IP addresses connected to websites that may display illegal content or even to take control of CSPs if deemed necessary to uphold the law.

(c) **Policies and Plans**

Digital health/E-Health legal and policy instruments

Rwanda has adopted a progressive attitude towards digital health, and has made notable achievements in the delivery of universal healthcare through leveraging digital health technologies. Rwanda's Fourth Health Sector Strategic Plan (2018–2023) is the latest health strategy developed by Rwanda and has four objectives: 1) full implementation of the main health programmes (improve demand, access and quality); 2) strengthen the health systems' building blocks (strengthen policies, resources, and management); 3) strengthen all levels of service delivery (organise the services effectively at all levels); and 4) ensure effective governance of the sector (strengthen decentralisation, partnership, private-sector coordination, aid effectiveness, and financial management).

Rwanda: National Disaster Management Policy, 2012

This policy seeks to establish the guiding principles and architecture for disaster risk management (DRM) in Rwanda by presenting the institutional structures, roles, responsibilities, authorities and key processes, in order to increase the resilience of vulnerable groups to disasters. A key policy action in the strategy is strengthening surveillance systems in relation to health epidemics, and this will involve use of geospatial data to develop early warning systems through routine surveillance and training in emergency operations.

National Contingency Matrix Plan

This is a strategic framework aimed at ensuring effective disaster risk management and response in the country. Geospatial data plays a crucial role in supporting the objectives of the plan by enhancing preparedness, response, and recovery efforts. Geospatial data may contribute to the aims of the National Contingency Matrix Plan in Rwanda as follows:

- *Risk assessment and mapping*:

  Hazard mapping: Geospatial data can be used to map areas prone to specific hazards. This information helps identify high-risk zones.
- *Vulnerability assessment*: Geospatial data can be used to assess the vulnerability of communities and infrastructure in different areas. This includes identifying populations at risk, critical infrastructure such as schools and hospitals, and areas with poor access to emergency services.
- *Early warning and monitoring*:

  Weather and climate monitoring: Geospatial data from weather stations and remote sensing satellites can provide real-time information on weather patterns and climate conditions. This is crucial for early warning systems to predict and prepare for weather-related disasters.
- *River and flood monitoring*: Geospatial data can be used to monitor river levels, rainfall intensity, and soil moisture, thus helping authorities to issue timely flood warnings and to evacuate at-risk communities.
- *Emergency response planning*:

  Resource allocation: Geospatial data can help identify suitable locations for emergency shelters, medical facilities, and supply distribution centres. It can also help optimise transportation routes for response teams.
- *Population density and movement*: Geospatial data can provide insights into population density and movement patterns, which are vital for estimating the number of affected people and planning evacuation routes.
- *Logistics and coordination*:

  Supply chain management: Geospatial data can be used to track the movement of relief supplies and resources, thus ensuring efficient distribution to affected areas.
- *Coordination of response teams*: Geospatial tools can help coordinate the efforts of multiple response teams by providing real-time situational awareness and location-based information.
- *Damage assessment and recovery*:

  Post-disaster damage assessment: After a disaster, geospatial data can be used to assess the extent of damage to infrastructure, housing, and agricultural land, thus helping to prioritise recovery efforts.

- Reconstruction planning: Geospatial data helps identify suitable locations for rebuilding infrastructure and housing, taking into account factors such as land suitability and accessibility.
- *Public awareness and education*:

  Interactive Maps: Geospatial data can be used to create interactive maps and visualisations that help raise public awareness about disaster risks and evacuation routes.
- *Training and simulation*: Geospatial data can support training and simulation exercises for response teams and communities, thus improving readiness for disaster events.
- *Policy and decision-making*:

  Evidence-Based Decision-Making: Geospatial data provides evidence and insights that support informed decision-making at all levels of government and among stakeholders involved in disaster risk management.

By integrating geospatial data into the National Contingency Matrix Plan, Rwanda can enhance its ability to prepare for, respond to, and recover from disasters effectively, thereby saving lives and reducing the impact of disasters on communities and infrastructure.

(d) Structures/Bodies/Organisations

Rwanda Spatial Data Hub

Geospatial data in the Rwanda Spatial Hub includes a wide range of information related to the country's geography, infrastructure, land use and natural resources. This data is collected, managed and maintained by various government agencies and organisations. Some common types of geospatial data that may be part of the Rwanda Spatial Hub include:

- Administrative boundaries
- Topographic data
- Land use and land cover data
- Transportation networks
- Natural resources data
- Infrastructure data

- Satellite imagery.

The availability and accessibility of geospatial data can vary based on the specific datasets and the policies of the organisations responsible for their management. Users should adhere to data usage terms and policies and stay updated on any changes or developments related to geospatial data in Rwanda.

National Spatial Data Infrastructure (NSDI)

SDI denotes the relevant base collection of technologies, policies, standards, and institutional arrangements necessary to acquire, process, store, distribute and improve the use of geospatial data from many different sources and for a wide group of potential users.

The National Spatial Data Infrastructure (NSDI) was envisioned as a way of enhancing the accessibility, communication and use of geospatial data to support a wide variety of decisions at all levels of society in Rwanda.

The goals of the NSDI Hub are to reduce redundancy in geospatial data creation and maintenance, therefore increasing resource efficiency, standardisation and informed decision-making. This Hub was launched as a national open platform to host and publish geospatial data and information relevant to sectoral planning and implementation.

The Hub contains mainly harmonised and standardised fundamental geospatial datasets from different institutions. It also hosts the Land-Use and development Master plans at national and Kigali City/District levels, and the recent topographic and thematic maps and story maps. The Rwanda Spatial Data Infrastructure was developed and managed by the Rwandan National Land Authority.

Centre for Geographic Information Systems and Remote Sensing (CGIS)

CGIS serves as a recognised multidisciplinary training and research centre of excellence in GIS and Remote Sensing technologies and applications. Through GIS and Remote Sensing, it addresses issues of local, national and regional importance, such as societal and economic transformation

and sustainable development in land administration, biodiversity conservation, sustainable urban planning, environmental management, and disaster risk management.

Rwanda Space Agency (RSA)

The RSA was established to develop Rwanda's space sector towards social-economic development. The mandate is to regulate and coordinate all space activities in the country while also creating an environment that encourages entrepreneurial and industrial development in order to enable the creation of commercialisation products that are globally competitive for local consumption and export markets. Other goals include developing and implementing capacity-building programmes in space sciences and technologies, and their applications, and developing highly skilled professionals in the space industry.

The RSA aims to coordinate Rwanda's space-sector activities towards securing communication, intelligence, surveillance and reconnaissance (ISR) and purchasing and playing a custodian role in national spatial data and imagery. As provided by the law establishing the RSA, some of its responsibilities include advising the government on creating and developing national and international space policies in order to implement the national and international space policies and strategies.

President Paul Kagame approved the draft law establishing the RSA. However, the Bill has not been approved.

Rwanda Allied Health Professions Council

Law No 46/2012 which established the Rwanda Allied Health Professions Council and determined its organisation, functioning, and competence, governs the health sector in Rwanda. It sets out the mission of the Health Council as being responsible for compliance with the rules, honour and dignity of the medical profession. The Council must ensure compliance with the principles of morality, integrity and dedication essential to the practice of the profession and must ensure that all its members comply with their professional requirements and the laws and regulations governing the medical profession.

Conclusion and Recommendations

The Rwandan government has established clear policy support for the use of geospatial data in pursuit of its ambitious aims in relation to digital health, space technology and disaster management response. Public–private partnerships have yielded a number of successful initiatives in these areas. Laws were lacking, but the enactment of a comprehensive data protection statute (DPP Law) brings Rwanda in line with modern data protection principles.

Clear guidance on legal compliance should be provided by regulators to encourage further research and innovation.

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 DPP Law, 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 DPP Law and to begin to assist users in navigating the DPP Law. It is not comprehensive, and users of the DPP Law 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 Rwanda, the Law on the Protection of Personal Data and Privacy (DPP Law) 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 to specifically 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 data for research purposes.

Health Research Regulations and Cross-Border Data Sharing

In addition to the national laws listed below, several international treaties and conventions have been signed. Of importance in this domain is the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention). Rwanda has ratified the Malabo Convention.

The relevant national legislation is Law No. 40/2017 Establishing the National Council for Science and Technology and determining its mission, organisation and functions, and also Rwanda FDA Law No. 003/2018. There are also numerous other laws, regulations and guidelines, including the:

- Health Sector Policy, 2015
- Health Sector Research Policy, 2012
- Law Establishing the National Cyber Security Authority and Determining its Mission, Organization and Functioning, 2017
- Ministerial Instructions No 003/2010
- Regulations governing the conduct and inspection of Clinical Trials in Rwanda
- Rules and Regulations for Research Activities (In accordance with the Ministerial Instructions No 003/2010 published in the official Gazette of the Republic of Rwanda Regulating research activities in Rwanda).

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

Law on Data Protection and Privacy

In addition to these legal and ethical requirements, the DPP Law applies to the processing of all personal data, and there are some special provisions in place for research. The conditions set out in the Law must all be met for research. 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 DPP Law are discussed below. Please note that this is not a thorough assessment of the DPP Law 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 Law on the Protection of Personal Data and Privacy

	Legal definition	**Layman explanation**
Data subject	A natural person from whom, or in respect of whom, personal data has been requested and processed.	This is the person to whom the data relates.
Data controller	A natural person, public or private corporate body or legal entity which, alone or jointly with others, processes personal data and determines the means of its processing.	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	Natural person, public or private corporate body or legal entity, which is authorised to process 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. He/she may be a consultant, for example.
National Cyber Security Authority		The independent body established to monitor and enforce compliance with the law
Data Protection Officer	Not defined in the DPP Law.	An individual in an organisation who is appointed to advise and promote compliance with the DPP Law.
Third party	Natural person, corporate body or legal entity other than the data	

	subject, data controller, data processor or persons who, under the authority of the data controller, are authorised to process personal data.	

Categories of Data listed in the Law on the Protection of Personal Data and Privacy

	Legal definition	Layman explanation
Personal data	Information relating to an identified or identifiable natural person who can be identified, directly or indirectly, particularly 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, psychological, genetic, mental, economic, cultural or social identity of that natural person.	Data about a particular person that can identify him or her.
Sensitive personal data	Information revealing a person's race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life, or family details.	Personal data that is sensitive for a particular person, such as health data and genetic data, and which receives additional legal protection.
Pseudonymisation	The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, which is kept separately.	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	No legal definition is provided.	Data where it is no longer possible to identify a person from it. It must not be possible to re-identify the person. Data protection law does not apply to anonymised data.

Generally, data protection law applies only to personal data. This is data that refers to an identified or identifiable person. For data that does not come under the definition of personal data, data protection law does not apply. The DPP Law applies specifically to "the processing of personal data".

The DPP Law refers to "de-identified" data and "pseudonymisation". Pseudonymisation is when information is removed from the data so that it is impossible to identify an individual, and that information is kept separate by using technical and organisational measures. Data that has been pseudonymised does fall under the DPP Law.

Although "de-identified" data is mentioned in the DPP Law, it is not defined. The DPP Law provides that it is an offence to knowingly, recklessly or intentionally re-identify data that has been de-identified. It appears from this context that de-identification is a reversible technique. It is unclear whether this data is exempt from the DPP Law. However, data that is not personal data does not fall under the DPP Law. Several types of data are considered personal:

- personal data;
- sensitive personal data (including genetic or biometric data);
- pseudonymised data;
- de-identified data.

The first three kinds of data (personal, sensitive personal (including genetic) data and pseudonymised data) are defined. An assessment would need to be made to consider whether data falls under these definitions. Unfortunately, given the lack of a definition for de-identified data, it is unclear what qualifies as de-identified data. Furthermore, whether pseudonymisation is merely a safety measure or whether it amounts to non-personal data in the hands of the data recipient who does not have access to the identifying data set is also unclear.

In the absence of a test or clear guidance from the Authority, the following is recommended from what can be clearly ascertained from the DPP Law and drawing on tests in other jurisdictions:

Recommended test - Ask yourself:

1. From the data, it is possible to individually identify a data subject, directly or indirectly, in reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual?
2. Can the data be linked with other data kept separately, in order to identify a data subject, either directly or indirectly?
3. Is the method used to de-identify the data subject reversible?
4. Is there any reasonably foreseeable method that could be used by someone to identify the data subject, directly or indirectly, by employing methods such as linking them to other data, or manipulating the data, or any other novel methods?

If the answer is "Yes" to *any* one of these questions, the data is *personal data* and will fall within the ambit of the DPP Law. If the answer is "No" to *all* of these questions, then this data will most likely be non-personal data and will fall outside the scope of the DPP Law.

Special Note Regarding Genetic and Genomic Data

Genetic data is considered to be sensitive personal data. It has a higher level of protection under data protection law. There is ongoing debate about whether genomic datasets can ever truly be considered not to be personal data, in particular as genetic data is an identifier. In its definition of genetic and biometric data, the DPP Law expressly provides that genetic data is sensitive personal data. Therefore, in deciding whether a genomic dataset can be considered to fall outside of the definition of personal data, context matters. Thus, consider whether data allows for anyone to identify the data subject.

Key Principles That Must be Met in Terms of the Law Relating to the Protection of Personal Data and Privacy

1. *Personal data is processed lawfully, fairly and transparently:* 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. The processing of sensitive personal data is generally not permitted unless it falls within one of the grounds in the DPP Law.
2. *Data is collected for explicit, specified and legitimate purposes and is 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. Therefore, the purpose must be clearly set out.
3. *Data is related to the purposes for which its processing was requested:* Only the data that is necessary for the specific purpose should be collected and processed. It is essential that only the minimal amount of data that is required to achieve the objectives of the data processing is used.
4. *Data is accurate and, where necessary, kept up to date, with every reasonable step being 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.
5. *Data is kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed:* Personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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.
6. *Data is processed in compliance with the rights of data subjects:* The data controller is responsible for, and must be able to demonstrate compliance with, the principles mentioned above. It is good practice to keep a record of data processing activities, measures introduced to protect the data, and any risk assessments made. This can be used to demonstrate compliance in the event of a breach.

Data Subject Rights in Terms of the Law Relating to the Protection of Personal Data and Privacy

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

(1) *Right to personal data:* The data subject has the right to request from the data controller information relating to the purposes of the processing of personal data and to access personal data that the data controller has about them. The data controller should have a process in place to facilitate this.
(2) *Right to rectification:* The data subject has the right to have inaccurate personal data corrected and incomplete data completed.
(3) *Right to erasure of personal data:* The data subject has the right to request that his/her data is erased. There is an exception where processing is necessary for the public interest or for historical, statistical, or scientific research.
(4) *Right to restriction of processing of personal data:* The data subject can request that the data controller stop processing his/her personal data.
(5) *Right to personal data portability:* The data subject has the right to move his/her data from one data controller to another.
(6) *Right to object:* The data subject can object to the processing of his/her personal data where the lawful basis of processing is not consent. This right can be deviated from if the data processor or data controller can show that there are legitimate reasons for the processing of personal data.
(7) *Right to not be subject to a decision based on automated data processing:* The data subject has the right to object to a decision based solely on automated processing. This right can be deviated from if the decision was based on the explicit consent of the data subject, the decision was necessary for the contract, or the decision was authorised by law and there are safeguards in place to protect the rights of the data subject.
(8) *Right to designate an heir to personal data:* The data subject has a right to designate an heir in his/her will who exercises rights when it comes to the processing of personal data.

Cross-Border Transfer of Personal Data

When considering the cross-border sharing of data for research, all the provisions of DPP Law must be met. The DPP Law also has a number of provisions on the cross-border sharing of data which, in addition to the other provisions, must be met.

Cross-border data sharing is not defined. It would apply when the data is being sent to a data controller/responsible party in another country. It *could* also include when a researcher outside of the country accesses the 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 or not is not yet settled law.

Lawful grounds for the cross-border flow of data

The possible lawful grounds for the cross-border flow of data are:

(1) The data controller or data processor must obtain authorisation from the supervisory authority after providing proof that the outside country has appropriate provisions;
(2) The data subject has provided his/her consent; or
(3) If the transfer is necessary for the performance of a contract between the data subject and data controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
(4) If the transfer is necessary for the performance of a contract between the data controller and third party that would benefit the data subject; or
(5) If the transfer is necessary for the public interest; or
(6) If the transfer is necessary for the establishment, exercise or defence of a legal claim; or
(7) If the transfer is necessary to protect the interest of a data subject or of another person where the data subject is physically or legally unable to give his/her consent; or
(8) If the transfer is for compelling legitimate interests pursued by the data controller or by the data processor and these interests do not override the interests, rights and freedoms of the data subject. This ground can apply only if the transfer is not repetitive and concerns only a limited number of data subjects, and the data controller or the data processor has

assessed all the circumstances of the data transfer and has, on the basis of that assessment, provided suitable safeguards for the protection of personal data; or

(9) The transfer is for the performance of international instruments ratified by Rwanda; or

(10) The supervisory authority can decide to add regulation determining another reason for sharing or transferring personal data to a third party outside Rwanda.

Contract for transfer of personal data

- In addition, if a data controller or data processor authorises a person to access personal data, or share or transfer the data to a third party outside Rwanda, he/she must enter into a written contract with such a person. This contract must set out the respective roles and responsibilities of each party to ensure compliance with the DPP Law.
- The supervisory authority may, by a regulation, determine the form of the contract to be used for transfer of personal data outside of Rwanda.
- The supervisory authority may also require the data controller or data processor to demonstrate their compliance with the provisions of the DPP Law and, in particular, with personal data security safeguards and interests referred to in the DPP Law.
- In addition, the supervisory authority may prohibit or suspend the transfer of personal data outside of Rwanda in order to protect the personal rights and freedoms of the data subject.

Storage of personal data outside of Rwanda

The storage of personal data outside of Rwanda is permitted only if the data controller or the data processor holds a valid registration certificate authorising him or her to store personal data outside of Rwanda, and such a certificate is issued by the supervisory authority.

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 dedicated legislation governs AI in Rwanda. 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

Rwanda has a SMART Rwanda Master Plan aimed at creating a knowledgeable society through SMART ICT. The Plan intends to secure national ICT execution capability, expand ICT accessibility, and establish programmes to enhance economic growth. Its focus will be on securing the adoption of ICT by upgrading protection and security, agreeing on rights and responsibilities for data use on the basis of context, and driving accountability and enforcement. The goal is to transform Rwanda into a regional ICT hub, therefore enhancing its reputation as a knowledge-based, middle-income nation.

Digital Health/E-Health

Rwanda's Fourth Health Sector Strategic Plan is its latest health strategy to ensure effective governance of digital health. The Law no 46/2012 establishes the Rwanda Allied Health Professions Council and determines its organisation, functioning and competence, which governs the health sector in Rwanda. Rwanda has a medical research facility known as the Rwanda

Biomedical Centre (RBC), which conducts scientific research and also provides care services to Rwandans.

From a practical perspective, the Government of Rwanda entered into a partnership with Babyl Health to enable all Rwandans to access quality healthcare services through their mobile phones, which then incorporate AI.

Medical devices

A Regulation governs control of the importation and exportation of pharmaceutical products and medical devices. It may be inferred from the definition of medical devices in the Regulation that AI could be included as a medical device.

Consumer Protection & ICT/E-Legislation

Consumer Protection	Law No 36/2012 relating to Competition and Consumer Protection
ICT/E-Legislation	Law No 058/2021 relating to the Protection of Personal Data and Privacy Law No 60/2018 on Prevention and Punishment of Cyber Crimes Law No 24/2016 Governing Information and Communication Technologies

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 DPP Law currently governs the processing of data in Rwanda. It provides that the data subject has the right not to be subject to a decision based on automated data processing such as profiling which may result in legal or alternative consequences for the data subject. However, this will not apply if the data subject has granted explicit consent, if it is necessary for the performance of a contract between the data subject and data controller,

and if the data controller is authorised by the law and there are specific measures in place to safeguard the data subject's rights, freedom and legitimate interests.

Other relevant provisions/definitions of the DPP Law are:

- *It defines pseudonymisation as the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, which is kept separately*. Defining pseudonymisation is progressive as maintaining confidentiality is another contentious debate, with one school of thought requiring genetic samples to be anonymised so that the data subject cannot be identified from the sample, and another not anonymising samples but rather coding them while retaining a high level of confidentiality. The Law also defines encryption and tokenisation, presumably to provide coverage to both sides of the above debate and this fills a possible legal lacuna in the data protection law.
- *It covers the sharing and transfer of personal data outside of Rwanda*. It requires that personal data be shared or transferred out of Rwanda only if the data subject has consented to this; if the data controller has obtained the relevant authorisations and provided proof of the necessary safeguards in place which will protect the personal data; and only for specific reasons such as the performance of a contract, the performance of international instruments, defending legal claims, and if it is in the interest of the public and the vital interest of the data subject.
- *The definition of 'consent of the data subject' requires specific consent.* In addition, a data subject's consent will be valid only if it was given freely with the full knowledge of possible consequences for granting such consent. A data subject also has the right to withdraw his or her consent at any time.

Intellectual Property

The Law No 31/2009 on the Protection of Intellectual Property governs intellectual property rights in Rwanda. One of the objectives of this Law is to disseminate technological knowledge to benefit the social and economic welfare of Rwanda's population. This objective may be in line with the advancement of AI in the medical sphere.

The Law defines computer program as "instructions expressed in words, codes, schemes or in any other form, which is capable, when incorporated in a medium that the computer can read, of causing a computer or any electronic device having information-processing capabilities to perform or achieve a particular task or result". This definition could be interpreted to include AI.

Developing AI to help provide medical services forms part of a human activity that produces a service and is therefore industrially applicable.

Summary and Analysis

While Rwanda has produced strategy/policy documents aimed at digital transformation and strengthening the ICT sector, these do not directly address AI regulation. Several policy documents guide digital health implementation, but no specific legislation provides for AI use in healthcare. However, AI may be included in the definition of medical devices. The above policy documents are interoperable and do not supersede one another. That said, relevant provisions in legislation take precedence over other regulatory/policy documents.

The DPP Law prohibits solely automated decision-making, which is important in AI regulation. AI technologies may receive some protection under Law No 36/2012 relating to Competition and Consumer Protection. However, the Law applies only to goods purchased for personal or domestic use. Furthermore, ICT/E-legislation and a consideration of intellectual property legislation, jurisprudence and soft law may be essential for ensuring that these technologies are properly used.