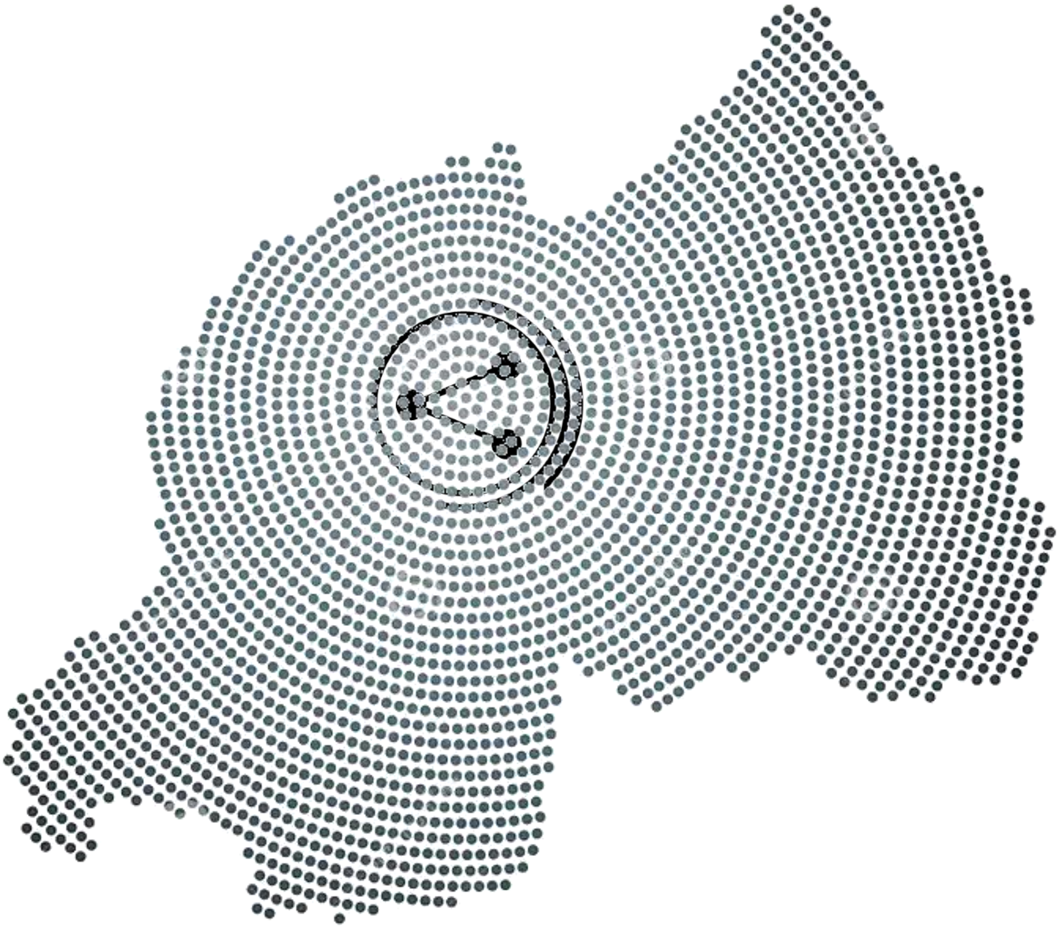
Republic of Rwanda

Ministry of ICT
and Innovation

The National Data Sharing Policy



MAY 2025

Acronyms, Abbreviations and Definitions

Access Control	Access control and management is a foundational principle in data management, information security and cybersecurity. It involves the application of policies, procedures and appropriate technologies. Every organization is required to ensure that data is only accessed by authorized persons. In the data sharing context, one of the objectives of the Data Sharing Principles is to ensure that data is only accessed by approved persons (see the principle 'Safe People').
API	**Application Programming Interface**. The Application refers to any software with a distinct function. Interface can be thought of as a contract of service between two applications. This contract defines how the two communicate with each other using requests and responses. Their API documentation contains information on how developers are to structure those requests and responses. The most commonly used APIs are REST (Representational State Transfer) or RESTful.
API Gateway	An **API gateway** is a modern architecture that supports interchange of information using APIs or microservices. The API Gateway acts as a front-end for API's, it receives API requests, supports throttling and security policies, and passes requests between a back-end service and requester. API Gateways offer developers a consistent interface to the many different ways APIs are implemented by their creators. API gateways are used for cloud services and are gradually replacing (or complementing) traditional ESB architectures.
Data	The word '**data**' refers to the representation of (what we assume are) facts through text, numerals, graphics, images, sound, or video. In the context of this policy document, data is seen as being digitally represented. Data has been called the "raw material of information" and Information has been called "data in context".
Closed Data	**Closed Data** refers to data that is considered highly confidential, sensitive, or secret information. It could include organization secrets, patents and intellectual property or information restricted by law. Sensitive could also be highly sensitive information (such as certain medical of data subjects which can never be shared). Access to such data is restricted to only certain parties within an organization. Closed data is deliberately not shared and does not fall under the scope of this Policy. This does not refer to personal data or other data shared for a valid lawful purpose.
DPPL	**Law N° 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy.** This law specifically applies to the processing Personal Data and its application in this policy is limited to instances where personal data is being shared and processed. It is referred to as the 'DPPL'.
DPO	**Data Protection Office** refers to the office of the Rwanda National Cyber Security Authority which fulfils the role of Data Protection Commissioner, or the

	'Supervisory Authority' as described in the DPPL[1], and enforces the requirements set out in the DPPL. The DPO spearheads all activities related to implementation of the DPPL to protect personal data and to guarantee of the privacy of individuals in Rwanda.
DPO (Controller or Processor in terms of DPPL)	Depending on the context, DPO also refers to the **Data Protection Officer** of an entity appointed in accordance with the DPPL[2] to ensure compliance to the DPPL and other responsibilities described in the law[3]
DGU	The Data Governance Unit, which will be established to provide governance and oversight of all data sharing activities.
DSP	The Data Sharing Platform – a digital platform built using modern, state-of-the-art technology architectures and world-class security mechanisms. The platform will be the vehicle which facilitates engagement and participation the data sharing between government entities.
ESB (also GESB)	An **Enterprise Services Bus** is a centralized software solution that connects services using a variety of protocols, data transformation technologies and routing of messages. Rwanda Information Services Authority (RISA) has implemented a Government ESB (GESB)
Information	**Information** refers to data that has been organized, structured, interpreted, or contextualized in a way that makes it meaningful and useful for a particular purpose. Where data consists of raw representations of observed facts (such as numbers, text, images, or sounds), information emerges when these data are processed to reveal relationships, patterns, or significance that support understanding, decision-making, or communication.
GoR	**Government of Rwanda**. This acronym refers to all institutions and agencies that make of up the government of Rwanda.
Open Data	**Open Data** is data that is made freely available and accessible to the public either (a) without restrictions or limitations on its use, reuse, or redistribution or (b) with some conditions such as measures that preserve provenance and openness or which may relate to licensing, attribution of sources etc.. Open Data is considered briefly in this document to provide context but does not fall within the scope of this Policy.

[1] Law N° 058/2021 of 13/10/2021 Relating to Data Protection and Privacy Chapter IV (Articles 27, 28) and other related responsibilities and powers as set out in the law.

[2] Law N° 058/2021 of 13/10/2021 Relating to Data Protection and Privacy Article 40..

[3] Law N° 058/2021 of 13/10/2021 Relating to Data Protection and Privacy Article 41.

Personal Data / Information	In this policy the term '**Personal Data**' has the same meaning as defined in the DPPL[4] It refers to any information that can be used to identify a living individual, either directly or indirectly. Personal data can include a wide range of information, such as names, addresses, phone numbers, email addresses, dates of birth, photographs, financial information, medical information, and social media activity.
Processing	The term '**Processing**' has the same meaning as defined in the DPPL[5]. Note that in the DPPL this term has application only for processing of 'personal data', but in the context of this policy, this term will apply to all data processed in the context of data sharing. Processing refers to any form of "access to, obtaining, collection, recording, structuring, storage, adaptation or alteration, retrieval, reconstruction, concealment, consultation, use, disclosure by transmission, sharing, transfer, or otherwise making available, sale, restriction, erasure or destruction". Any personal or sensitive data that is shared in terms of this policy is considered to be processed and therefore compliance with the DPPL is required..
Sensitive Data	In this policy the term '**Sensitive Personal Data**' has the same meaning as defined in the DPPL[6]. It refers to "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 life". Other data, which is not personal data, may be considered 'sensitive' by a participating entity under this policy and may be subject to restrictions.
Statistical Data:	For the purposes of this policy, **Statistical Data** shall have the meaning assigned to it under Law No. 05/2013/OL Relating to the Organization of Statistical Activities in Rwanda. It includes numerical data held by the National Statistical Institute of Rwanda, originating from surveys, censuses, or other research activities, whether processed or unprocessed. Statistical Data shall fall within the scope of this policy only insofar as its inclusion aligns with the provisions of Law No. 05/2013, particularly the confidentiality requirements stipulated in Chapter VI therein.
Shared Data and Data Sharing	**Shared Data** refers to data that is made available for use by multiple persons, systems, or applications- within one organization or shared with another. In the context of this policy '**Shared Data**' refers to information shared by one government institution for use by another, under the strict guidelines and requirements as set forth in this Policy and 'Data Sharing' is the act of sharing

[4] Law N° 058/2021 of 13/10/2021 Relating to Data Protection and Privacy Article 3(1).

[5] See Law N° 058/2021 of 13/10/2021 Relating to Data Protection and Privacy Article 3(4).

[6] See Law N° 058/2021 of 13/10/2021 Relating to Data Protection and Privacy Article 3(2).

	such information between government institutions. Such data could include information that has been aggregated, de-identified or is purely statistical in nature. *It may, however, include personal or sensitive information if such sharing complies with legal requirements and is necessary to fulfil a legal or government objective*
TSC	Technical Subcommittee of the DGU. This subcommittee will act as the technical arm of the DGU to ensure compliance with technical requirements, guide development of key technical components and fast-track data sharing activities which are already established.

Table of Contents

INTRODUCTION 3

SITUATION ANALYSIS 4

POLICY CONTEXT 5

POLICY SCOPE OF APPLICATION 9

POLICY AREAS AND ESSENTIAL COMPONENTS 9

POLICY IMPLEMENTATION PLAN 12

POLICY SUMMARY

The National Data Sharing for Government policy aims to ensure that data is shared in a protected and well governed manner between agencies of the GoR to enhance decision making, facilitate collaboration and provide the basis for fulfilling national policy objectives and facilitating digital transformation for the benefit of citizens of Rwanda.

Key objectives are to facilitate the free flow of information without creating unnecessary obstacles and to promote data innovation and solutions to complex development challenges while meeting any concerns related to data protection and privacy and regulatory compliance.

POLICY OBJECTIVES

Promote Evidence-Based Policy Making

Increasing the availability and use of public sector data provides evidence about the effectiveness of government programs and allows for informed decisions on new approaches or changes to existing programs.

Create Transparency and Accountability

Data sharing in government improves transparency and trust while promoting the core principles of human rights and protection of personal information.

Protect Privacy and Confidentiality

Responsible, governed data sharing ensures that institutions have a clear understanding of which data is sensitive, what may be shared and what may not (and therefore protected vigorously).

Promote Collaboration

Data sharing between government agencies can facilitate inter-agency collaboration and the development of coordinated approaches to addressing complex issues.

Improve Efficiency and Innovation

By allowing different government agencies to access and share data, it is possible to eliminate duplicative efforts and streamline processes, leading to cost savings and improved efficiency government services delivery.

Create Opportunities for Self-Service

Government agencies can improve their own analytical and decision-making capabilities as they become less reliant on outcomes from other analytical sources but are able to interrogate the raw data themselves.

Enhanced Decision-Making and the Ability to Define New Areas of Benefit

Data from multiple sources can provide a more accurate and complete picture of a given situation, which can inform better policy decisions.

Often the true value of data lies not just in the data created or collected within one sector, but in being able to overlay or 'mashup' data from one sector with that which has been shared by another sector Examples, could be (1) overlaying transport data with demographic data and spending patterns for transport transactions in mobile money data will help policymakers understand which routes are most efficient, or the lack of spending data may indicate where routes are inefficient or do not exist or (2) using agricultural data interlinked with spatial data to identify to improve crop yields, planting and irrigation, fertilizer use and more.

Avoid an Overly Reactive Approach to Regulatory Requirements

By providing guidance and knowledge-based processes, along with assistance for legal requirements such as Privacy Impact Assessments (PIA) and Data Sharing Agreements, government agencies are better equipped to implement the requirements of the Personal Data Protection Law.

INTRODUCTION

Data is a national asset and the way it is used can significantly impact the welfare of the nation.

Data produced or collected by government sectors and agencies is essential for measuring the effectiveness of public sector and delivering citizen-centric public services, policy development and evaluation, and various other government operations. The value in data sharing between government institutions lies in the ability to use the data for meaningful insights that benefit the national interest. Where there is a reluctance to share information, or perceived barriers to sharing, this results in siloed efforts, duplication of effort and an inability to explore opportunities for new and innovative uses of data to further national interests and benefit Rwanda's citizens.

This National Policy for Data Sharing between Government Agencies considers the reasons for data sharing, the essential components of a platform for data sharing and key principles and procedures that must be adhered to.

SITUATION ANALYSIS

Data sharing between government entities has been formally established in many countries around the world. This has been done because of a clear understanding of both the **necessity and the benefits** to national interests of such a policy of freely sharing data in protected and well governed environment.

In preparing this policy, several international examples were considered, particularly where there has been

(I) Clear policy or policy definitions,
(II) Established structures for oversight and governance and protection of data in compliance with data protection regulations,
(III) Establishment of appropriate technologies and standards to ensure that data sharing is based on modern, secure platforms and (iv) dedicated resources for ongoing development and monitoring of the various aspects of the data sharing processes.

Among the countries and international bodies considered, were:

- Singapore
- Australia
- New Zealand
- England
- United States of America
- South Africa
- The European Union

There are many lessons to be learned from these international examples[7]. Among these are (1) that a united national approach, as set out in this policy, is essential to ensure the success of data sharing initiatives and (2) that the most successful implementations are built on strong governance and a modern, secure technology architecture.

Additionally, the passage of Law N° 058/2021 Relating to Data Protection and Privacy (the 'DPPL') has raised concerns among certain parties as to whether they should be sharing certain data and under what circumstances they may or may not be permitted to share such data. Another objective of this policy is to create the environment where data sharing data between government entities is managed within a set of principles built on clear oversight and guidance, good governance, compliance with regulation, world-class security, and state-of-the-art technological enablement.

[7] A primary example of how data can be used for national benefit is set out in the Productivity Commission Inquiry Report into Data Availability and Use (2017) which led to the establishment of Australia's Data and Transparency Act of 2022

POLICY CONTEXT

This data sharing policy for government establishes the guidelines and procedures to facilitate the secure and responsible sharing of data between different government agencies or departments. The policy aims to provide a standardized approach to data sharing, while ensuring that data privacy and security are maintained. It builds on the foundation laid by other policies and strategies and bases its guidance on regulations and policies which have been implemented or are being developed. The table below sets out some of the policies and regulations considered:

Policy or Regulation	Impact on Data Sharing
Data Revolution Policy	Now expired, the Data Revolution policy provided for technological innovation in the use of data and analytics to grow the Rwanda economy and benefit its citizens. It proposed, among other things, the practices of Data Sharing among government institutions and Open Data. It also proposed the formation of a National Data Steering Committee.
ICT for Governance (or ICT4_GOV) Cluster Strategy 2020-2024	Provides guidance on Interoperability and Data Sharing between government entities.
Law N° 058/2021 of 13/10/2021 Relating to Data Protection and Privacy (the 'DPPL')	The DPPL protects all personal and sensitive information. It is referenced frequently as a primary guidance for data sharing. It establishes, among other things, the legal bases for processing, fair processing principles, rights of data subjects, the establishment of a Supervisory Authority (the NCSA) and various requirements for Controllers and Processors.
Law N° 24/2016 of 18/06/2016 Governing Information and Communication Technologies (ICT Law)	A comprehensive legislation that governs the use of information and communication technologies in Rwanda. It covers wide range of subject areas and application in specific sectors. It does not deal directly with data sharing, but addresses aspects of data protection and cybersecurity, which are aligned with the provisions of this policy.
Law N° 05/2013/OL of 16/06/2013 on the Organization of Statistical Activities in Rwanda	Relating to the Organization of Statistical Activities in Rwanda - Governs the organization of statistical activities in Rwanda and the protection of confidential statistical data.
Law N° 04/2013 of 08/02/2013 Relating to Access of Information	This law provides for disclosure of information by public bodies that is in the public interest. While the focus is on provision of information to the public and journalists, the principles of sharing data are seen as complimentary to this policy, which focuses on sharing between government institutions.
Law N° 60/2018 of 22/08/2018 on Prevention and Punishment of Cybercrimes	This law deals with cybercrimes and unlawful access to restricted information and the associated remedies and penalties. It aligns with the principles in the DPPL dealing with unlawful access of personal data ('personal data breach'). The principles of controlled access and security align with the governance principles proposed in this policy.

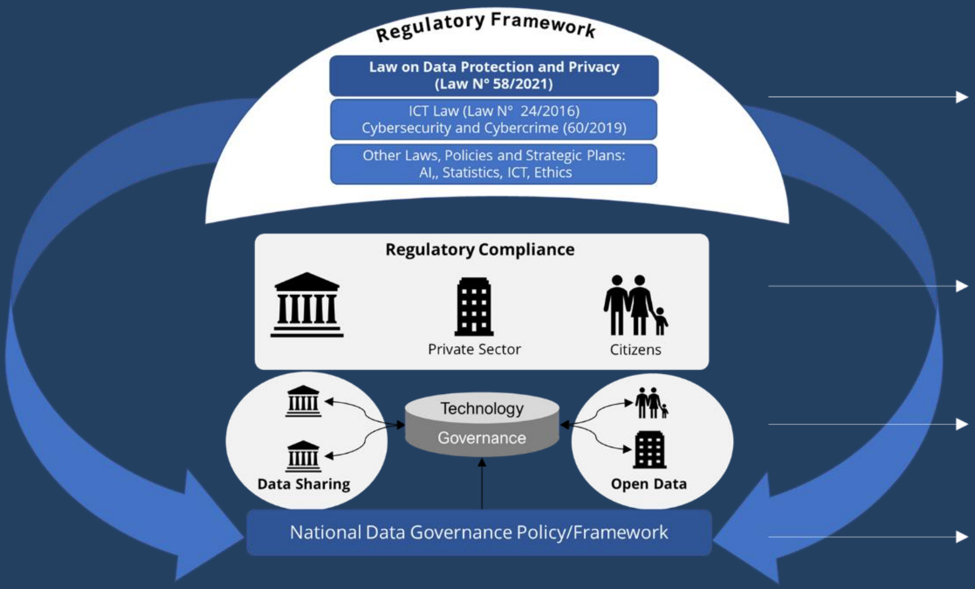
Cybersecurity Policy and Laws	In addition to the laws noted above, several other instruments exist that provide regulation and guidance for cyber security measures. These include the Cyber Security Policy of 2015, the RISA Directives on Cyber Security for Network and Information Systems for Public Institutions of 2018 and the RURA Cybersecurity Regulation N˚ 010/R/CR-CSI/RURA/020 of 29/05/2020. Each of these establishes requirements and good practices for implementing appropriate cyber security measurements in government institutions or regulated bodies.
Other considerations	It is envisaged that considerations focused on the ethical use of data and technologies such as Artificial Intelligence (AI) and Machine Learning (ML) will have an influence on data sharing. This includes the Rwanda National AI Policy. This Data Sharing policy will be adjusted as needed to cater for these and other emerging technologies or risks.

Table 1: Some Policies and Regulations considered in the Data Sharing Policy

INTERPLAY BETWEEN DATA SHARING, OPEN DATA AND REGULATION

All data in government, whether it is data that will be 'Shared' or is considered 'Open', are subject to the same requirements of governance and compliance with applicable regulation, such as the DPPL. This means that information must be identified and defined, complete, of high quality and classified to ensure that it is appropriately protected and shared.

The diagram below illustrates the interplay between the components of Data Sharing and Open Data with regulatory requirements and the technology and governance requirements to facilitate these:


Regulatory Framework
Law on Data Protection and Privacy (Law N° 58/2021)
ICT Law (Law N° 24/2016) Cybersecurity and Cybercrime (60/2019)
Other Laws, Policies and Strategic Plans: AI,, Statistics, ICT, Ethics
Regulatory Compliance
Private Sector
Citizens
Technology
Governance
Data Sharing
Open Data
National Data Governance Policy/Framework

National Regulations and Policies provide the overarching compliance framework

All data users must comply with applicable laws

Data shared between government institutions or made publicly available will flow through a governed digital platform

All GoR institutions must implement Data Governance

Figure 1 – Interplay between regulation, data governance and data sharing initiatives
(Source: Cenfri)

This policy focuses on Data Sharing, i.e., the act of sharing data (which can include sensitive or personal information) between government departments and agencies. It establishes the principles behind sharing such data among government institutions in a well-governed manner to eliminate data silos in government and to facilitate the protected used of such data to further Rwanda's national objectives and to better serve its citizens by delivering services that are simple and effective, respectful, inform better government policies and programs, and support world-leading research and development.

It further has the objective of removing, as far as possible, hurdles and challenges which reduce the ability to derive the best use and value from data in public sector institutions. It aims to do this by establishing the foundation of clearly defined technology architecture for data sharing that incorporates strong safeguards, along with consistent, efficient processes which operate under the auspices of entrenched principles of governance.

These proposed measures are designed to reduce or eliminate common barriers by establishing common technical and governance standards and processes, which must exist not just in the data sharing arena, but within each entity which participates in the sharing of public sector data.

By applying the principles and actions described in this policy, it will be possible for government departments and public bodies to align data sharing systems and processes and embed data sharing as a strategic priority across government.

POLICY ORIENTATION

This data sharing policy for government establishes the guidelines and procedures to facilitate the secure and responsible sharing of data between different government agencies.

Vision

The vision of this policy is to optimize the use of data to further Rwanda's goals of being a smart nation through safe sharing of data between government agencies.

Mission

The mission of this policy is to promote the free flow of protected data between government entities within a well-governed, secure environment, based on the data sharing principles, which allows these organisations to collaborate to achieve national objectives and use data to promote the innovative use of data for the national good.

Objective

The primary objective of this policy is to enable government entities to share data in the national interest under a protected, secure, and well governed framework.

Guiding Principles

This policy is founded on the following primary principles:

(1) Regulatory Compliance – all data sharing complies with all regulatory requirements.
(2) Protection, Governance and Oversight – Data sharing will take place within a framework of clearly defined mechanisms to ensure data protection, governance, and oversight. This includes the establishment of a Data Governance Unit and Data Sharing Agreements between participating entities and the application of the Data Sharing Principles.
(3) Secure, modern technological enablement – the platform that facilitates the sharing of data is built on secure, modern international best-practice technologies.
(4) Standards and Quality – data shared between government entities will conform to define standards and will be of high quality.

POLICY SCOPE OF APPLICATION

This policy applies to all data sharing activities between GoR entities or agencies.

POLICY AREAS AND ESSENTIAL COMPONENTS

This data sharing policy for government establishes certain essential components for data sharing between government entities to ensure that:

(1) Data Sharing is well-governed with clearly defined oversight structures and rules of engagement.

(2) Data Sharing is well-defined and complies with established standards.

(3) Data Sharing complies with regulatory requirements, is secure and adheres to internationally recognized risk management principles.

(4) Data Sharing is enabled by a world-class technology architecture incorporating state-of-the-art technology and security features.

Policy Component 1	**Governance and Oversight**

Governance and oversight are essential components of data sharing in all countries across the world where data sharing has been formalised across the world. This policy places the obligation on each entity to ensure that any data shared is well governed within that organisation. Refer to *Annex 6* for an overview of these obligations.

The policy also aims to establish The Data Governance Unit, along with its Technical Subcommittee. Refer to *Annex 1* which defines the structure, role, and terms of reference of the DGU and TSC.

Together, these will oversee data sharing activities and ensure that there is a formal approval process and the conclusion of a data sharing agreement between participating entities. Please refer to *Annex 2* for a template of the Data Sharing Application form, *Annex 3* for a template of the Data Sharing Agreement and *Annex 4* for a high-level overview of the process to be followed.

Policy Component 2	**Defined Standards**

The Data Governance Unit shall define an approved standard for data that is to be shared in accordance with this policy.

Policy Component 3	**Regulatory Compliance, Security and Risk Management**

Any data sharing activities must comply with regulatory requirements, most notable being the Law N° 05/2013/OL Relating to the Organization of Statistical Activities in Rwanda and the Law N° 058/2021 Relating to Data Protection and Privacy (referred to as the 'DPPL'). While the latter does not prohibit the free flow of personal information for government or legal purposes, it places the burden on bodies sharing information to do so responsibly and in accordance with all the requirements for processing personal information lawfully. Similarly, other laws also govern what data may be shared and conditions that may apply, as noted under 'Policy Context'.

Supporting this law will be other legal and policy instruments that address cybersecurity, the ethical use of artificial intelligence (AI) and other principles such as adherence to a framework for the governance of data.

The DPPL, in Article 47, requires any organisation that is 'processing' personal or sensitive data, either as a Controller or a Processor, to ensure that have 'appropriate, reasonable measures' in place These measures must include:

- Registration with the Supervisory Authority as a Controller or Processor (or both).
- Internal policies and procedures that clearly articulate the organisation's standards and procedures for managing personal information.
- Risk Assessments and risk management and mitigation procedures.
- Regularly verifying the effective implementation of safety and security measures
- Update measures in response to new risks identified.

This policy aims to ensure that ALL data that is shared between government entities is processed securely by establishing a secure platform for such transfers. It still requires each entity participating in data sharing to ensure that it has applied its own appropriate security safeguards within the organization.

Finally, this policy requires that entities participating in data sharing follow the Data Sharing Principles See *Annex 5* for a discussion of these principles and how they should be applied.

Annex 6 further provides a high-level view of the responsibilities of government entities participating in data sharing as defined in this policy.

Policy Component 4 Technology Platform

A primary objective of this policy is to ensure that data sharing is not unnecessarily encumbered by slow, manual processes or poorly defined transfer mechanisms. Consequently, this policy aims to establish a dedicated platform, built on modern, state-of-the-art technology and world class security practices.

This platform will facilitate the full process of engagement between entities participating in the data sharing activity, from initial application, through approval by The Data Governance Unit or its Technical Subcommittee, through to establishing of Data Sharing Agreements and finally the transfer of data via secure API technology.

The platform, fronted by a rich web interface or portal, will allow government entities to understand what information is already available via the platform and provide guidance on what procedures to follow from application through to fulfilment.

The platform will include constant monitoring of activities across all aspects of cybersecurity as well as providing clear metrics to inform The Data Governance Unit and other stakeholders of how well the platform is performing and where issues exist.

IMPLICATIONS OF POLICY IMPLEMENTATION

Governance and Oversight

The Ministry of ICT will be responsible for providing policy guidance and oversight for the implementation of this policy.

All government entities that participate in the national data sharing for government programme must ensure that their data is well governed within their organisation. This means that data must be understood, be complete and of high quality and must be protected.

Additionally, each participating entity will need to register on the data sharing platform as well as register its legal signatories for electronic signing of data sharing agreements.

A Data Governance Unit will be established by ministerial order, along with its Technical Subcommittee. Their composition, mandate and terms of reference are clearly defined and are attached hereto as Annex 1.

Annex 1 provides further information on approvals. In summary, requests for data sharing will be:

1. Automatically approved for unrestricted data that is already available through the DSP.
2. Approved by authorized parties (such as CDOs) where approval is not automated or restricted data is being requested.
3. Reviewed in exceptional circumstances by the DGU where authorization is denied, or special circumstances arise.

The data sharing technology platform will include monitoring components which will provide additional information for oversight such as service levels and throughput, availability, issues regarding compliance with standards or service delivery etc.

Financial Implications

To achieve the objectives and targets identified in this new policy, an estimated budget of RWF 10 billion will be invested, primarily funded by the government.

The implementation of this new policy will cater for efficiency and optimized use of data assets, leading to enhanced uses of data through advanced analytics to improve decision making and create opportunities for new uses of data. This will lead to greater opportunities for funding and investment in the Rwanda economy, spur economic development and entrench Rwanda’s goals of being the innovation hub of Africa insofar as the use of data is concerned.

POLICY IMPLEMENTATION PLAN

No.	Policy Component / Area	Target	2025	2026	2027	2028	2029	Responsible
	Policy Component 1: Governance and Oversight							
1	Establish Data Governance Unit-ministerial approval	DGU is established with clearly defined membership, mandate, roles, terms of reference and ministerial powers. *(Annex 1)*	🟨					MINICT, RISA, NISR, NCSA.
2	Establish Technical Subcommittee (TSC) of the DGU	The TSC has defined membership, roles, and responsibilities. *(Annex 1)*	🟨					MINICT, RISA, Member agencies
3	Implement 'appropriate organisational and technical' security safeguards	All government entities have demonstrable data and cyber security policies and technologies in place	🟨	🟨	🟨			All entities, led and guided by MINICT, RISA, NCSA.
	Policy Component 2: Defined Standards							
4	Define and confirm data standards for data sharing, including data classification	A defined set of data standards is approved and made available to all entities participating in data sharing as a prerequisite	🟨	🟨				MINICT, NISR, RISA, external consultants
	Policy Component 3: Regulatory Compliance, Security and Risk Management							
5	Define National guidelines for Data Governance (framework)	A documented framework is available to all institutions for implementing data governance, to ensure consistency.	🟨	🟨				MINICT, NISR, RISA, external consultants
6	Institute programs for data governance and	All government entities implement a data strategy that incorporates data governance, primary component	🟨	🟨	🟨	🟨	🟨	All entities, led and guided by MINICT, RISA
7	Institute programs for data protection & privacy to demonstrate compliance with the DPPL	All government entities have implemented a privacy program and can provide evidence of compliance	🟨	🟨	🟨	🟨	🟨	All entities, led and guided by DPO Office of NCSA. MINICT to provide support.
8	Implement 'Data Sharing Principles	Government entities participating in data sharing will implement data sharing principles for risk management	🟨	🟨	🟨	🟨	🟨	All entities, led and guided by MINICT, RISA
	Policy Component 4: Technology Platform							
9	Establish technical team and project for creation of the Data Sharing Platform (DSP)	A secure platform for data sharing exists, created using state-of-the-art technology architectures exists.	🟨	🟨	🟨			MINICT, RISA
10	Create technical and functional requirement specifications, including SLAs	The DSP will include core functional capabilities defined by RISA, the DGU and TSC and other stakeholders	🟨	🟨				Technical Task Team, DGU, TSC, RISA, other stakeholders

Policy Component 4: Technology Platform (Continued)									
11	Build DSP according to specification	The technical task will build a fit for purpose modern platform to facilitate data sharing	🟨	🟨				Technical Task Team, TSC, RISA
12	Create online portal for registration and use of data sharing platform	A dedicated, secure portal exists where entities can register, discover existing shared data sets, submit new applications, and confirm data sharing agreements	🟨	🟨				Technical Task Team, TSC, RISA
13	Implement monitoring and reporting mechanisms	The DSP must have continual monitoring and reporting capabilities to ensure SLAs are met and issues are resolved,	🟨	🟨				Technical Task Team, TSC, RISA
14	Ongoing improvements to the DSP as required	The DSP is continually enhanced according to requirements or to address issues highlighted through monitoring	🟨	🟨	🟨	🟨	🟨	Technical Task Team, TSC, RISA
15	Assist with creation of APIs and other mechanisms to utilize the DSP	The technical task team, under guidance of the TSC, will assist entities to create APIs and other mechanisms needed to participate in data sharing via the DSP		🟨	🟨	🟨	🟨	Technical Task Team, TSC, RISA
16	Ongoing education and assistance to participating entities	All government entities have access to training and awareness delivered via the DSP portal or other means		🟨	🟨	🟨	🟨	TSC, MINICT, RISA
17	Use of Data Sharing Platform for all data sharing activities	All data sharing activities and engagements are conducted via the DSP, governed by the DGU	🟨	🟨	🟨	🟨	🟨	All entities participating in data sharing