

## Overview of the National Policy on Data and Cloud 2024

South Africa’s first national policy on data and cloud services was published on 31 May 2024. The [National Policy on Data and Cloud 2024](#) articulates the approach that the South African government will take to the collection, storage, use, and sharing of data and the use of cloud technologies.

What is the aim of the Policy? .....	1
Digital infrastructure .....	1
Access to Data and Cloud Services.....	2
Creating a Digital Trust Environment .....	2
Cross-Border Data Transfers and Data Sovereignty .....	3
Skills and Capacity Development .....	3
Competition in the Data and Cloud Market.....	4
Research and Development (R & D).....	4
Governance and Institutional Mechanisms .....	4
Implementation .....	5

---

### What is the aim of the Policy?

To ensure that data is utilized to drive innovation, economic growth and improved public services, while maintaining stringent standards for data security and privacy, through:

- Outlining key enablers for cloud adoption and utilization to drive digital transformation and digital economic inclusion
- Creating a safe and secure environment for digitization and digitalization
- Ensuring transparency by data and cloud service providers in the provision of their services to citizens
- Providing for appropriate governance arrangements

The Policy applies to all levels of government, state organisations and private entities and persons.

---

### Digital infrastructure

The Policy recognises that it may not be feasible for government to own and manage data centres with its limited resource base: services will need to be obtained from the private sector.

Policy proposals and interventions focus on energy supply, skills, data-sharing and systems interoperability to provide a degree of regulatory clarity to the private sector on meeting government’s procurement needs.

### Policy interventions

- Government departments and entities shall prioritize cloud services as the primary option for new ICT procurement.
- Government data shall be stored in unified, cloud-enabled data centers, facilitating data-sharing, interoperable systems, scalability, and cost optimization. This infrastructure will be supported by redundancies in designated locations to meet business continuity requirements.
- The [Minimum Information Security Standards \(MISS\)](#) – to be updated - will be the guiding framework for access to government data (to be monitored by SITA).
- SITA is responsible for sourcing data infrastructure and cloud services for government, including developing and monitoring service level agreements that guarantee consistent, reliable, and secure data and cloud services.
- SITA must also drive adoption of digital government services, applications, and solutions.
- All data centres in South Africa:
  - must be built and operated in adherence to environmental legislation and building by-laws
  - must not be built in restricted areas such as heritage sites, national key points, or land designated for land reform
  - must not be located in areas prone to natural disasters or social disturbances
  - must display / provide verifiable certification credentials to all potential customers
  - must prioritise the self-provision of electricity and water
- Data centres used by the government should comply with a fault-tolerant design that provides a minimum uptime of 99.995%.

---

### Access to Data and Cloud Services

This aspect of the Policy focuses on adopting frameworks which facilitate access to government and private sector data, unlocking the value of this data for industry and others. The Policy emphasises that the value of data is maximised when it is made available in a timely, consistent, accurate, complete, unique and valid manner.

### Policy Interventions

- All government data must be captured in or converted to digital format.
- All government data in digital format must be classified into the following categories: public | open data | confidential/sensitive data | secret | top secret.
- An Open Data Framework must be adopted to enable access to government data.
- Data protection legislation must be complied with.
- Government wants to create a free basic connectivity grant to indigent and other qualifying households to ensure that they can exercise their ability to access data.
- Access to data must not expire.
- All data classified as public or open must remain accessible.

---

### Creating a Digital Trust Environment

Government acknowledges that it bears the responsibility of creating an environment that makes consumers confident in using of digital technologies and platforms. This requires a secure and safe online environment with effective mechanisms for redress.

**Policy Interventions**

- Data protection authorities must be adequately resourced and capacitated to discharge their functions.
- All digital technologies used by the government should incorporate cybersecurity-by-design principles, covering the entire lifecycle of data collection, processing, use, storage, mining, and destruction.
- Government must prioritize the signing and ratification of regional, continental, and global treaties and conventions supportive of collaboration in fighting cybercrimes.
- Cloud providers should be transparent about their credentials and provide detailed information, licenses, and certificates.

---

**Cross-Border Data Transfers and Data Sovereignty**

The Policy recognises the importance of cross-border data transfers and the negative consequences of unwarranted restrictions, particularly for commerce and multinationals. It emphasises the need for a framework for inter-government data sharing as an element of initiatives such as the African Continental Free Trade Area (AfCFTA).

**Policy Interventions**

- The processing of data collected within South Africa must comply with local data protection and security laws and policies, including POPIA.
- Government data incorporating content pertaining to the protection and preservation of national security and sovereignty shall be stored only in digital infrastructure located locally.
- The government shall pursue cross-border data transfers and sharing agreements that:
  - Promote national interests, including socio-economic development, security, and sovereignty
  - Comply with local data protection and data security laws and policies
  - Enhance mutually beneficial cooperation for all parties involved
  - Give effect to the AfCFTA, Southern African Customs Union, Single Digital African Market, and AU and SADC protocols

---

**Skills and Capacity Development****Policy Interventions**

- Government must develop an adaptable strategy for skills development and retention.
- School syllabi must incorporate digital literacy and technologies across the learning ecosystem and fund this sufficiently.
- Skills surveys must consistently be taken in the sector to align interventions with requirements.
- The National School of Government and other partners must develop and adapt digital skills programs to ensure the adoption and usage of digital technology across government.
- International agreements shall prioritize unemployed youth and graduates, women, and people with disabilities.
- The Minister must only support accredited Equity Equivalent Investment Programmes skills interventions which prioritize youth, unemployed graduates, SMMEs and rural women.

## Competition in the Data and Cloud Market

The Policy identifies a concentration of ownership of local data centres and cloud service providers and proposes interventions intended to remedy this.

### Policy Interventions

- The Competition Commission shall conduct studies in the data centre and cloud services markets to identify potential anti-competitive trends and behaviour, and where applicable, identify proactive preventative measures to ensure a fair and competitive market.
- Cloud service providers shall ensure transparency regarding data portability and interoperability costs and technical implications at the point of contracting, to help customers to make informed decisions and promote fair competition.
- Competition among and investment in data and cloud service providers shall be encouraged to foster competitive and innovative offerings, as well as to potentially reduce costs for consumers.
- Different architectures and operating systems shall be supported to provide a variety of options for the public, ensuring that consumers have access to diverse and suitable technological solutions.

---

## Research and Development (R & D)

### Policy Interventions

- The Department of Science and Innovation (DSI), in collaboration with the Department of Communications and Digital Technologies (DCDT), shall be responsible for research and development (R&D) on big data and cloud computing, in alignment the White Paper on Science, Technology, and Innovation.
- The government shall increase R&D spending with a focus on supporting innovation and technology development. The Technology Innovation Agency shall be adequately funded and capacitated to support South African innovators.
- Academia, research institutions, industry and innovation hubs must collaborate with government in R&D, exploiting new technologies to build world-class data centres and cloud capabilities.

---

## Governance and Institutional Mechanisms

The Policy provides for establishing an Advisory Council and, importantly, obliges SITA to develop the processes governing government acquiring data centre and cloud services from the private sector.

### Policy Interventions

- The Minister is to establish an Advisory Council comprising public and private representatives to:
  - Co-ordinate initiatives and investments in data centres and cloud technologies
  - Enhance data management standards, guidelines, best practices and the use of data for innovation and economic activities
  - Provide technical support and assistance, including awareness programmes
  - Contribute to developing a regulatory framework for managing of data and cloud services
  - Strategic data sets that can stimulate innovation, the economy and support service delivery

- Development of an Interoperability framework between government and other key stakeholders
- Sector-specific regulators, supported by policy from relevant departments, shall develop regulatory frameworks to support the cloud and data-based digital technologies and technology adoption in their specific sectors.
- The DPSA shall develop norms and standards on data and cloud services for the Public Service. These norms and standards shall not supersede existing legislative powers vested in other State organs in terms of data management.
- SITA shall develop guidelines and technical standards for the acquisition and operations of data centres and cloud services to ensure that government obtains the best affordable service in the market.
- A Data and Cloud Technical implementation Task team is to be formed comprising key government stakeholders such as DCDT, the SSA, Treasury, DPSA and Home Affairs.

---

### Implementation

The policy will be implemented through consultations with key stakeholders and implementing agents such as SITA, relevant government departments, governance bodies and where necessary industry and sector stakeholders.

---