DEPARTMENT OF COMMUNICATIONS AND DIGITAL TECHNOLOGIES

NOTICE 2533 OF 2024

ELECTRONIC COMMUNICATIONS ACT 2005
(ACT NO. 36 OF 2005)

PUBLICATION OF THE FINAL NATIONAL DATA AND CLOUD POLICY

I, Mondli Gungubele, the Minister of Communications and Digital Technologies, following Cabinet approval on 27 March 2024, hereby publish the final National Data and Cloud Policy in line with section 3(1) of the Electronic Communications Act (Act No. 36 of 2005) ("ECA").

Mr. Mondli Gungubele, MP

Minister of Communications and Digital Technologies

communications
& digital technologies
Department:
Communications & Digital Technologies
REPUBLIC OF SOUTH AFRICA

NATIONAL

POLICY ON

DATA AND CLOUD

2024

Table of Contents

ABBREVIATIONS

AfCFTA	African Continental Free Trade Area
CRSA	Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996).
CCA	Cybercrimes Act, 2020 (Act No. 19 of 2020)
CDT	Communications and Digital Technologies
COVID-19	Coronavirus Disease 2019
DCDT	Department of Communications and Digital Technologies
DPSA	Department of Public Service and Administration
DSI	Department of Science and Innovation
ECT	Electronic Communications and Transactions, Act, 2002 (Act No. 25 of 2002)
GB	gigabyte
GDPR	General Data Protection Regulation (European Union Regulation)
GITOC	Government Information Technology Officers Council
ICT	Information and Communication Technology
IT	Information Technology
ITU	International telecommunications Union
IaaS	Infrastructure as a Service
IDC	International Data Corporation, 2018
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
MICT SETA	Media Information and Communication Technologies Sector Education and Training Authority
MISS	Minimum Information Security Standards (1996)
NARSSA	National Archives and Record Service of South Africa Act, 1996 (Act No. 43 of 1996)
NCPF	National Cybersecurity Policy Framework
NGOs	Non-Governmental Organizations
NEMISA	National Electronic Media Institute of South Africa
NICIS	National Integrated Cyber Infrastructure System
NIST	The National Institute of Standards and Technology
OECD	Organisation for Economic Cooperation and Development
PAMA	Public Administration Management Act, 2014 (Act No. 11 of 2014)

PaaS	Platform as a Service
POPIA	Protection of Personal Information Act, 2013 (Act No. 4 of 2013)
RICA	Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002
R&D	Research and Development
SaaS	Software as a Service
SACU	Supporting Southern African Customs Union
SDIA	Spatial Data Infrastructure Act, 2003 (Act No. 54 of 2003)
SEZs	Special Economic Zones
SITA	State Information Technology Agency
SMMEs	Small, Medium and Micro enterprises
SSA	State Security Agency
Stats SA	Statistics South Africa
UNCTAD	United Nations Conference on Trade and Development
WOAN	Wireless Open Access Network
4IR	Fourth Industrial Revolution

1. EXECUTIVE SUMMARY

The National Data and Cloud Policy is a framework aimed at efficiently managing and utilizing data through cloud computing technologies. Its primary goals are to enhance government service delivery and foster socio-economic development by promoting data-driven decision-making and creating data-based tradable goods and services, thereby supporting an emerging digital economy.

Key principles of the policy include:

1.1 Accelerating the rollout of digital infrastructure to ensure fast, secure, and reliable broadband connectivity.
1.2 Ensuring data privacy and security.
1.3 Promoting open data and data interoperability.
1.4 Adopting a cloud-first approach.

The policy also underscores the importance of capacity building and skills development to encourage the adoption of cloud technologies and data management practices across all sectors. It aims to create a robust data economy that contributes to the growth of the ICT sector and the overall economy.

Aligned with the government's digital transformation agenda, the policy is expected to catalyze the development of a data-driven ecosystem in the country. Its implementation is anticipated to yield benefits such as improved public service delivery, increased government operational efficiency, better data management, and enhanced innovation and competitiveness in the private sector. Successful implementation will require collaboration among multiple stakeholders, including government agencies, the private sector, civil society organizations, and international partners. Adequate funding, stakeholder engagement, and capacitation of the State Information Technology Agency (SITA) will be critical for the policy's success.

2. INTRODUCTION

The South African economy, like other economies, is digitising rapidly. This means that citizens and consumers, from both the private and public sectors, will access most of the services on digital platforms through electronic devices. Government and private sector organisations are transforming their service delivery models, shifting them towards digital

domains, ensuring that citizens and customers can access the services securely at any given time, anywhere, and from any device.

The digital domain is becoming essential for economic efficiency. Cross-border trade is increasingly facilitated by the internet and e-commerce platforms, which enable scalable implementations through extensive ecosystems. Digital platforms facilitate easy collaboration with other ecosystem partners.

The COVID-19 pandemic exacerbated social and economic challenges in South Africa but also highlighted opportunities created by digital transformation and the digital economy to address these challenges.

South Africa’s ability to effectively address its socio-economic challenges will depend significantly on how it leverages the digital economy's opportunities. This can be achieved through policy frameworks that harness the economic and social potential of data and cloud computing. Such frameworks should be citizen-centric, support existing government initiatives for universal access and affordability, and address challenges related to digital infrastructure, devices, software, applications, and digital skills.

Data's greatest advantage is the value it generates when processed through digital technologies. However, the capacity to transform data into meaningful insights is largely confined to major technological companies in developed countries. Data facilitates communication between machines, smart devices, individuals, businesses, and government entities. Therefore, South Africa must develop the capacity to fully exploit the opportunities presented by a data-driven economy.

Recognizing data as a strategic asset and enabler for the digital economy is crucial. Government, academic institutions, non-governmental organizations, and industry regularly generate high volumes of data. By 2025, it is projected that the total amount of digital data created worldwide will rise to 163 zettabytes, driven by the growing number of devices and sensors (International Data Corporation, 2018). This implies a significant investment in data storage and processing to derive value from it.

The digital economy's growth and expansion rely on the use and adoption of various digital technologies. Implementing strategies, policies, and legislative measures to exploit these technologies for data processing and analysis will enable the development of digital goods

CONTINUES ON PAGE 130 OF BOOK 2

Printed by and obtainable from the Government Printer, Bosman Street, Private Bag X85, Pretoria, 0001
Contact Centre Tel: 012-748 6200. eMail: info.egazette@gpw.gov.za
Publications: Tel: (012) 748 6053, 748 6061, 748 6065

Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID AFRIKA

Vol. 707 31 May Mei 2024 No. 50741

PART 2 OF 2

ISSN 1682-5845
9 771682 584003 50741

and services. This will address service delivery challenges and economic inclusion, making South Africa globally competitive.

To fully benefit from the digital economy, investment in broadband infrastructure, data centres, and associated technologies such as cloud computing is necessary. Such investments should be supported by clear IT security protocols, cybersecurity measures, and a data governance framework that supports open data principles.

The overall policy framework on data and cloud must be based on open standards and systems, including open-source frameworks, rather than closed and exclusive systems. The integrity of a digital economy, as a sharing economy, depends on its ability to deliver sharing advantages to ecosystem partners while protecting citizens, customers, and partners.

3. PROBLEM STATEMENT

Government departments and agencies collect vast amounts of data related to services such as health, education, identity documents, birth registration, driver's licenses, and business registrations. This data is stored in various formats, with some kept as hard copies and others in servers within departmental facilities.

The private sector, in contrast, has rapidly digitized, using digital technologies like data analytics and cloud services to gain insights for customizing products and services and identifying new opportunities.
The government faces challenges due to slow technology adoption, leading to disjointed data collection, storage, and processing. The lack of common data governance mechanisms hampers data integration, sharing, and system interoperability. This siloed approach results in lost opportunities for evidence-based policymaking, integrated planning, and making non-sensitive data available for innovation and the development of digital goods and services to support employment and reduce poverty.

Considering data as a key enabler for digital transformation and the digital economy, it is crucial to ensure equitable access to data to foster digital and economic inclusion. In a society marked by significant inequalities (South Africa had the highest income inequality in 2021 with a Gini score of 63), the government must continually seek mechanisms to foster economic inclusion and bridge the gap between the rich and poor. Digital inclusion through affordable connectivity, data, and digital technology access is vital for achieving these goals,

especially for small, medium, and micro enterprises (SMMEs) and startups, which have the potential to create jobs and contribute to economic growth.

Digital inclusion should also focus on the indigent, the youth, women and people with disability to enable them, not only to be able to access government services, but to also have access to data and internet connectivity to enable them to innovate and develop digitally tradable goods and services necessary to ensure their economic inclusion. Ultimately, any reference to the digital economy must be supported by strong, reliable, secure and affordable connectivity to affordable digital infrastructure and devices.

The private sector and other organisations have started using technologies in high numbers. This means there is increased investment in digital technologies such as data centres and cloud services. The sharing of data between the government and the private sector can have a significant impact on the improvement of services offered by both parties, thus benefitting the citizens. The absence of a regulatory environment might deter increased investment in digital technologies as investors largely seek regulatory certainty to ensure adequate protection of their investments.

Connectivity and utilisation of technologies should be supported by a reliable energy supply. South Africa has over time experienced energy supply challenges which has had a negative impact on government and industrial initiatives to grow the economy and foster economic inclusion. The functionality of most of the digital infrastructure relies significantly on reliable energy supply. Data centres also rely significantly on cooling systems that require vast volumes of water. In addition to energy supply challenges, issues of sustainability are beginning to take centre stage. The implication for South Africa is that in its pursuit of reliable energy supply solutions, consideration should be given to ensuring that data centre providers ensure that they make self-provisioning for water and electricity self-provisioning while addressing carbon emission reductions to mitigate against environmental degradation.

In a global and digitally connected world driven by free data inflows and outflows, there is already a realisation that some countries establishing regulatory mechanisms to protect certain types of data regarded as critical for their security and sovereignty. In addition, there is also a recognition that data-sharing across different jurisdictions can also be beneficial to country economies. Collaborative economic developmental initiatives like the African Continental Free Trade Area, (ACfTA), the African Single Digital market and digital identity will rely significantly on data-sharing within different jurisdictions. All these initiatives must be

supported by a regulatory regime that creates confidence, consistency, certainty and reliability.

A data and technology-driven economy and digital transformation involve significant online activities and interactions. Major cyber-attacks that happened in South Africa in 2019 caused disruptions and significant economic harm. Although South Africa is ahead of its African counterparts in terms of data security and protection, there is still a need to ensure that appropriate institutional mechanisms are in place and institutions vested with protecting and securing South African data and cyberspace are adequately resourced and capacitated.

Availability of digital infrastructure, affordable connectivity and technology adoption would be meaningless in a society where there is no capacity to convert such enablement into meaningful economic activity. Many ICT stakeholders are involved in digital skills capacity development initiatives, but these initiatives are not adequately addressing digital skills shortages and gaps. By implication South African skills interventions alone are not having the required impact on digital skills shortages. To address digital skills shortages therefore requires a deliberate, focused, integrated and collaborative approach which seeks to maximise available scarce resources to achieve a greater impact.

The Data and Cloud policy seeks to enable a pathway for citizens to derive socio-economic value out of data so that they can be able to participate in an inclusive digital economy. It also seeks to reinforce government's digital technology adoption, specifically cloud enabled data storage and processing solutions, to enhance service delivery and evidence based policy-making. The policy further recognises that South Africa is part of a globally connected and digitally transformed and transforming community and should therefore not only assert its data sovereignty rights, but also adopt a cross-border data transfer regime that enables collaborative partnerships with regional, continental and other global partners.

The policy further recognises the need for digital capacity enablement and creating a secure cyber-environment that not only protects companies and citizens from cyber-threats, but also creates a digital trust environment which will encourage and support investments necessary to create a robust and sustainable digital economy.

4. RATIONALE FOR THE DATA AND CLOUD POLICY

As technology advances, businesses are increasingly utilizing cloud services to store and process their data. However, this shift towards the cloud has created new challenges in terms of data security and privacy. Due to the increasing reliance on digital technologies and the need to protect sensitive data, a comprehensive Data and Cloud policy is crucial for any organization looking to use cloud services.

In recent years, South Africa has seen exponential growth in the use of digital technologies, increasing the volume of data generated. The country has recognized the importance of cloud computing in driving digital transformation. The government has implemented policies to promote the adoption of cloud technologies. The Cloud First Strategy has been developed to prioritize cloud services for all new IT projects and encourages public sector organizations to use cloud services to improve efficiency.

The exponential growth in data has created a need for more dynamic storage solutions, which cannot be met by traditional computing systems. Data centers and cloud technology can provide solutions to problems associated with the storage and processing of large quantities of data.

The digital economy is experiencing exponential growth, propelled by advancements in cloud computing technologies that facilitate the gathering, analysis, and synthesis of extensive digital data. The Presidential Commission on the 4th Industrial Revolution asserts that broadband internet and data are foundational to the digital economy, and that reliable, accurate, standardized, integrated, and easily accessible citizen data is critical for building e-government services across sectors such as health, transport, and justice.

Countries are developing strategies and policies to fully exploit the opportunities presented by data and cloud computing to build create digitally transformed societies and strong digital economies. To this effect, there is an emerging trend to prioritise the promotion of data as a strategic asset and countries are implementing data protection laws and policies, such as the European Union’s General Data Protection Regulation (GDPR).

The implementation of this policy will benefit the country as follows:

- Enhanced data security: - the policy will protect private and sensitive information from cyberattacks through the establishment of data protection protocols as required by the Protection of Personal Information Act, 2013 (POPIA).
- Digital transformation - the policy will promote the use of technology in different sectors to increase productivity and efficiency.
- Improved public service delivery – The policy will promote the use of cloud-based solutions, which will help government departments offer better services to citizens and businesses.
- Economic growth – the policy will enable more businesses to leverage technology, which will lead to increased job creation and economic growth.
- Enhanced collaboration – The policy aims to facilitate enhanced collaboration among government departments, private entities, and research institutions, fostering the exchange of knowledge, data, and expertise.

5. OVERVIEW OF THE POLICY, LEGISLATIVE AND REGULATORY LANDSCAPE

South African data legislative history was marked by the protection of state secrets and protect the sanctity of information. This begun with the Protection of Information Act of 1982 (Act No. 84 of 1982), the National Archives and Record Service of South Africa Act of 1996 (Act No. 43 of 1996), and the Minimum Information Security Standards (MISS) of 1996. These measures were conceived in an era where the digital economy was a distant dream, ensuring that sensitive state information remained in trusted hands.

With the dawn of democracy in 1996, enshrined in the Constitution of the Republic of South Africa (Act No. 108 of 1996), the right to privacy was elevated to a constitutional guarantee. Section 14 of the Constitution proclaimed that every individual had the right to:

- Their person or home searched.
- Their property searched.
- Their possession seized.
- Their person or home searched.
- Their property searched.
- Their possession seized.
- The privacy of their communications infringed.

As the new millennium approached, South Africa's democracy matured, heralding a new era of transparency. The passage of the Promotion of Access to Information Act of 2000 (Act No. 2 of 2000) (PAIA) signalled a pivotal shift. This act empowered citizens to scrutinize government decisions, ensuring accountability and fostering an open society.

By 2002, the digital revolution had begun to reshape the landscape. Recognizing the need for secure online transactions, the Electronic Communications and Transactions Act of 2002 (Act No. 25 of 2002) (ECT) was enacted. This legislation aimed to safeguard electronic dealings, shielding them from subversive and fraudulent activities, thus bolstering citizen trust in digital platforms.

Simultaneously, the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA) was introduced to protect against arbitrary interceptions of communication, upholding the right to privacy in the digital age.

The digital transformation continued unabated, and in 2003, the Spatial Data Infrastructure Act (Act No. 54 of 2003) (SDIA) was passed. This act underscored the importance of spatial information in planning, marking a recognition of data as a crucial tool for governmental operations.

As digital transactions proliferated, the necessity for a secure cyber environment became paramount. By 2012, the National Cybersecurity Policy Framework was developed, acknowledging the cyber threats that could undermine national security and economic stability. The subsequent Cybercrimes Act of 2020 (Act No. 19 of 2020) (CCA) was a direct response to these emerging threats, providing a robust legal framework to combat cybercrime.

In parallel, the Protection of Personal Information Act of 2013 (Act No. 4 of 2013) (POPIA) was enacted to safeguard personal data in an increasingly digital world, ensuring that personal information was protected from exploitation and misuse.

Recognizing the need for integrated information management, the Public Administration Management Act of 2014 (Act No. 11 of 2014) (PAMA) was introduced. This legislation aimed to enhance interoperability across government systems, fostering seamless information sharing and collaborative governance.

The National Integrated ICT Policy White Paper of 2016 marked a watershed moment, acknowledging the economic value of data. This policy highlighted the potential of data to drive innovation and support digital economic inclusion, emphasizing the importance of data sharing under stringent privacy protections.

Despite these advancements, the primary focus of South African legislation largely remained on data protection and security. Except for the 2016 White Paper, there has been a lack of legislative efforts to create an enabling environment for a digital, data-driven economy. The need for a comprehensive policy and regulatory framework that supports broader access to data for innovation in digital services and products remains necessary.

The National e-Government Strategy and Roadmap hinted at the transformative potential of a cloud ICT architecture. This strategy envisioned interoperable government ICT systems, enabling efficient service delivery and integrated management across governmental departments.

In conclusion, these legislative and policy developments must be viewed in the context of the National Development Plan. This plan calls for South Africa to enhance its global presence, boost competitiveness, attract investment, and drive economic growth through innovation and technological advancement. The journey towards a robust digital economy is ongoing, and the legislative landscape must continue to evolve to support this vision.

6. LEGISLATIVE CONTEXT

As a rapidly developing nation on the African continent, South Africa has recognized the transformative potential of advanced technologies such as cloud computing to propel its economy and enhance the quality of life for its citizens. However, with these technological advancements come a host of challenges, including cybersecurity risks, data privacy concerns, and the imperative for robust policies and regulations. In response, the South African government has implemented a comprehensive framework of policies and regulations to govern cloud computing and data usage.

One of the most pivotal policies in this arena is the National Integrated ICT Policy White Paper, published in September 2016. This policy aims to create a conducive environment for the deployment, adoption, and utilization of ICTs across South Africa. It underscores the necessity for heightened cybersecurity measures, the promotion of local data storage

solutions, and the development of regulations that ensure data privacy and advocate for ethical data usage.

Complementing this, the Protection of Personal Information Act (POPIA), enacted in 2013, enforces the constitutional right to privacy by regulating the processing, collection, and storage of personal information by both public and private entities. POPIA is designed to safeguard the personal information of individuals, ensuring it is handled responsibly and securely.

To bolster the country's cloud data privacy and cybersecurity regulations further, the South African government has initiated a review of its National Cybersecurity Policy Framework (NCPF), initially released in 2012. This review aims to update the framework to address contemporary cybersecurity threats and challenges, ensuring its continued relevance and effectiveness. The country's data protection laws work in tandem to protect personal information, while the National Data and Cloud Policy seeks to guarantee the secure and reliable storage of data in the cloud.

The development of the National Data and Cloud Policy is informed by a broad spectrum of legislation, policies, procedures, guidelines, and other documents related to data and cloud computing, including:

6.1. Protection of Information Act No. 84 of 1982
6.2. Minimum Information Security Standards (MISS), 1996
6.3. National Archives and Records Service of South Africa Act, Act No. 43 of 1996 (NARSSA)
6.4. Promotion of Access to Information Act, Act No. 2 of 2000 (PAIA)
6.5. Electronic Communications Act, Act No. 36 of 2005
6.6. Electronic Communications and Transactions Act No. 25 of 2002 (ECTA)
6.7. Spatial Data Infrastructure Act, Act No. 54 of 2003 (SDIA)
6.8. National Cybersecurity Policy Framework, 2012
6.9. Protection of Personal Information Act, Act No. 4 of 2013 (POPIA)
6.10. Public Administration Management Act, Act No. 11 of 2014 (PAMA)
6.11. National Integrated ICT Policy White Paper, 2016
6.12. National e-Strategy, 2017
6.13. Cybercrimes Act, 2020 (Act 19 of 2020) (CCA)

6.14. The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA)

6.15. DPSA Determination and Directive on the Usage of Cloud Computing Services in the Public Service

Through this comprehensive legislative framework, South Africa aims to foster a secure, efficient, and innovative digital environment that supports both governmental and economic objectives, ensuring that the nation can harness the full potential of cloud computing and data technology.

7. POLICY STATEMENT

This policy articulates the government's comprehensive approach and guidelines for the collection, storage, use, and sharing of data. It also outlines strategies for leveraging cloud technologies to enhance government services and bolster the growth of the digital economy. By establishing clear principles and practices, this policy aims to ensure that data is managed securely and ethically, while promoting innovation and efficiency within the public sector. The ultimate goal is to create a robust framework that supports transparency, protects privacy, and fosters economic development through the strategic use of digital and cloud technologies.

8. PURPOSE

This policy aims to enable South Africans to realize the socio-economic value of data, outlining the government's policy position on cloud-based long-term data storage and compute requirements. It also establishes the necessary governance mechanisms to support these initiatives. By doing so, the policy seeks to ensure that data is utilized to drive innovation, economic growth, and improved public services, while maintaining stringent standards for data security and privacy.

9. AIM

The Policy aims to establish consistency and predictability in the adoption of data and cloud technologies by both the government and South African citizens. It seeks to:

9.1 Outline key enablers for cloud adoption and utilization to drive digital transformation and digital economic inclusion.

9.2 Create a safe and secure environment for digitization and digitalization.

9.3 Ensure transparency by data and cloud service providers in the provision of their services to citizens.

10. OBJECTIVES

The policy aims to create an enabling environment for the use and provision of data and cloud services to ensure socio-economic development and inclusivity. The specific objectives of this policy are to:

10.1 Promote connectivity and access to data and cloud services.
10.2 Address the government's long-term data storage and processing requirements.
10.3 Create a Data Trust environment through data privacy protection and cybersecurity measures.
10.4 Promote standardization of compliance in respect of data and cloud computing.
10.5 Provide clarity on cross-border transfers and data sovereignty.
10.6 Ensure consumer protection in the use of data and cloud services.
10.7 Establish institutional mechanisms for the governance of data and cloud services.
10.8 Support the development of Small, Medium, and Micro Enterprises (SMMEs).
10.9 Facilitate capacity development to enable and expand the use of data and cloud services.
10.10 Encourage research, innovation, and human capital development.

11. SCOPE

This policy applies to:

11.1 National and Provincial government.
11.2 Organs of State/Public Enterprises.
11.3 Private Sector.
11.4 General public/individual citizens.
11.5 Data Controllers and Data Custodians.

12. DEFINITION OF CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services) that

can be rapidly provisioned and released with minimal management effort or service provider interaction".

13. CLOUD COMPUTING SERVICE MODELS

Cloud services are primarily provisioned using three traditional models – IaaS, PaaS, and SaaS. These service delivery models differ in how responsibility and accountability are shared between the cloud service provider and the consumer of the cloud-provided services.

13.1. Software as a Service (SaaS)

In the SaaS model, cloud users directly access the applications provided by the cloud provider. This model offers the convenience of not having to manage the underlying infrastructure or the capabilities of the applications, allowing users to focus solely on utilizing the software.

13.2. Platform as a Service (PaaS)

PaaS provides users with a more structured platform to deploy their own applications and services. Users can rely on the programming languages and additional tools provided by the cloud provider to develop, deploy, and manage applications without handling the underlying infrastructure.

13.3. Infrastructure as a Service (IaaS)

IaaS offers fundamental computing resources such as processing power, storage, and networks to cloud users. This model enables users to leverage these resources through their own implementation of virtualization capabilities, providing the flexibility to manage and control the infrastructure according to their specific needs.

14. CLOUD DEPLOYMENT MODELS

Cloud services are provisioned using the following deployment models. Each of these has advantages, disadvantages and constraints.

14.1. Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.

Private cloud services are more expensive than public cloud services because they require hardware, software, licenses and maintenance. The cloud computing customer will need the hardware, operating system and licenses for software applications.

14.2. Public cloud

The cloud infrastructure is provisioned for open use by the public. It may be owned, managed, and operated by a business, academic, government organisation, or some combination of them. It exists on the premises of the cloud provider. It operates in a public and shared environment and is less costly. Examples of public cloud are Amazon, Google, Azure, Microsoft Office 365, Gmail and Dropbox.

14.3. Hybrid cloud

Employs both private and public infrastructure such that a section of the data centre is reserved for a single tenant, and the remainder is available to the public. Hybrid clouds are typically employed when only part of the data is supposed to be outsourced to keep full control of sensitive data and, at the same time, take advantage of higher flexibility through outsourcing.

15. POLICY INTERVENTIONS AND PROPOSALS

15.1. Digital infrastructure

Digital Infrastructure refers to the underlying technological foundation that supports digital services, processes, and applications. This infrastructure includes hardware systems, software systems, networks, and communication systems. Cloud Computing is a type of digital infrastructure that enables users to access and utilize computing resources and services over the Internet, including servers, storage, databases, software, and networking tools.

The National Integrated ICT Policy White Paper, 2016 sets forth measures to ensure the rapid deployment of electronic communication infrastructure. The proposed policy intervention on digital infrastructure aims to bridge the digital divide, ensuring universal access to cloud and data infrastructure services for all South Africans. This policy intervention is closely linked to other inclusion strategies, such as South Africa Connect / National Broadband Policy, which seeks to ensure all South Africans have access to broadband services by 2030.

South Africa is home to data centre investors and cloud providers with global reach, competencies, and experience, providing efficient and affordable data storage and processing facilities due to economies of scale acquired over years of operation. However, the government faces limited resources and increasing citizen needs, necessitating a balance between both against finite financial resources. While there might be sentiments favoring government-built data centers for full control, the prohibitive costs associated with building, running, and maintaining these facilities could render them unsustainable and impractical, potentially becoming white elephants in a few years.

Currently, South Africa faces electricity supply challenges. Given that data centers operate 24 hours a day and consume vast amounts of electricity, reliance solely on the national grid may be insufficient. Therefore, it is crucial for data centre owners and operators to implement additional alternative energy resources to prevent operational disruptions.

The establishment and operation of data centers require specialized technical skills, which may not be widely available in South Africa at present. Even where such skills exist, the government must compete with the private sector, with its limited funding, to attract these skilled professionals.

Given these challenges, it may not be feasible for the government to own and manage data centres with its limited resource base.

Data-sharing across government departments has proven invaluable in enabling the government to provide integrated support services during times of disaster, such as during the Covid-19 pandemic, when different government departments had to collaborate to deliver integrated services to citizens. This data-sharing can also support integrated planning and evidence-based policies and services, assisting the government in providing comprehensive support to citizens from birth to old age. For instance, data-sharing by the Departments of Health, Education, Social Development, and Home Affairs can ensure that upon birth, a child is immediately registered in the birth register and acquires a birth certificate and identity number from Home Affairs. With a record of the number of children born in a particular year, the government can plan for their education, social support, and infrastructure needs in advance based on empirical data. This approach can also aid law enforcement by enabling tracking and tracing based on citizen records, such as fingerprints. Therefore, data storage and processing infrastructure must facilitate data-sharing and systems interoperability.

Lastly, data and cloud service providers need regulatory clarity to guide their investment. This regulatory clarity is provided by policies and legislation that outline compliance requirements for infrastructure rollout and performance standards, specifically for the government. Due to water and electricity supply constraints and the high demand for these resources by data centres, data centre hosts and suppliers should have water and electricity backup to avoid service disruptions and reduce pressure on the grids. The government may need to develop incentive schemes to encourage water and electricity conservation by data center operators.

Policy interventions

15.1.1. Funding, technical, and other related resources shall be galvanized towards achieving the target of 100% broadband coverage by 2030 to ensure broadband access for all South Africans.

15.1.2. 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.

15.1.3. The State Information Technology Agency (SITA) shall be the responsible authority, by virtue of its legislative mandate, to source data infrastructure and cloud services for the government. SITA will ensure the development and monitoring of service level agreements that guarantee consistent, reliable, and secure data and cloud services for the government. To this end, the government should ensure that SITA is adequately capacitated and resourced to fulfil its responsibilities.

15.1.4. The Minimum Information Security Standards (MISS) shall be the guiding framework for access to government data in unified government data centers and will be updated to align with technology-driven computing. Organizations such as the South African Revenue Services (SARS) and Statistics South Africa (StatsSA) shall retain their data access governance requirements in accordance with their legislation.

15.1.5. In line with the e-strategy, SITA shall drive the adoption of digital government services, applications, and solutions, with respective national and provincial departments running and managing their own applications.

15.1.6. All data centres in South Africa shall be required to comply with the following:

15.1.6.1. Data centres must be built and operated in adherence to environmental legislation and building by-laws.

15.1.6.2. Data centres must not be built in restricted areas such as heritage sites, national key points, or land designated for land reform.

15.1.6.3. Data centres must not be located in areas prone to natural disasters or social disturbances.

15.1.6.4. Data centres must display or be able provide verifiable certification credentials to all potential customers.

15.1.6.5. Data centres used by the government should comply with a fault-tolerant design that provides a minimum uptime of 99.995%.

15.1.6.6. Priority should be given to the self-provision of electricity and water for the operations of data centres to ensure continuous operation and reduce dependency on the national grids.

Policy Proposals

15.1.7. Digital infrastructure connectivity must be provided on a universal access service basis and facilitated by both government and private infrastructure providers on a non-discriminatory basis.

15.1.8. Government data shall be stored in a unified cloud-enabled data center, enabling data-sharing, interoperable systems, scalability, and cost-optimization. This infrastructure shall include redundancies in designated locations to meet business continuity requirements, ensuring consistent and reliable access to critical data.

15.1.9. The State Information Technology Agency (SITA) shall be the responsible authority for sourcing data infrastructure and cloud services from industry providers for the government. SITA shall develop and monitor service level agreements to guarantee consistent, reliable, and secure data and cloud services. Additionally, SITA will monitor access to government data through the Minimum Information Security Standards (MISS) and drive the implementation of the government's e-Strategy.

15.1.10. Government departments and entities shall prioritize cloud services as the primary option for new ICT procurement.

15.1.11. Data center operators shall ensure the provision of their own electricity and water supply as backup for their energy and cooling requirements.

15.2. Access to Data and Cloud Services

Data possesses several critical features that provide opportunities for socio-economic development and inclusion. The government, as a repository of vast volumes of data from various sectors, is uniquely positioned to offer complete, high-quality, and reliable data for use by SMMEs, startups, and industry, while ensuring compliance with privacy protection requirements. This necessitates the development and adoption of frameworks to make government data available to different sectors of society.

A significant portion of government data remains in paper form due to the slow pace of technology adoption and a lack of resources. To enable meaningful processing, this data needs to be converted into digital formats.

The private sector also amasses substantial volumes of data through its transactional relationships with customers, which include citizens, organizations, institutions, and other companies. When made available and utilized, this data can help derive insights that drive innovation, foster creativity in problem-solving, and facilitate the development of new and tradable digital goods and services.

If the government and private sector collectively pool their data to ensure accessibility to all, while ensuring compliance with privacy protections, such data can create a robust foundation for a digital and data-driven economy. Importantly, it can significantly contribute to the development of evidence-based policies and strategies by the government and ensure that its service delivery programs are responsive to diverse and unique citizen needs. In summary, access to both government and private sector data can:

- Enhance innovation and creativity in problem-solving.
- Facilitate the development of new digital goods and services.
- Support the creation of evidence-based policies and strategies.
- Ensure responsive and efficient government service delivery.

For data to be truly valuable, it must be timely, consistently available, accurate, complete, unique, and valid. This ensures that the data can be effectively used to drive socio-economic development and foster inclusivity.

Policy Interventions

15.2.1. All government data shall be captured in or converted to digital format. The services of primarily SMMEs should be sourced and utilized for this work, promoting local business involvement and fostering economic growth.

15.2.2. An Open Data Framework shall be developed to enable access to timely, accurate, complete, consistent, and valid government data for SMMEs, startups, citizens, and industry players. Access to such data shall comply with existing data protection policies and legislation, ensuring privacy and security are maintained.

15.2.3. A Data for Development Framework shall be established to facilitate the availability of timely, accurate, complete, consistent, and valid private sector data to the government, supporting service delivery. This data shall also be accessible to SMMEs, startups, and citizens to drive innovation and the development of digital solutions and tradable digital goods and services. The availability of such data shall comply with data protection laws and policies.

15.2.4. To promote digital economic inclusion, the government shall allocate resources and capacity to enforce universal service obligations. This will ensure that indigent communities, unemployed youth and graduates, and people with disabilities have access to free connectivity, enabling them to access online government services and digital platforms.

Policy Proposals

15.2.5. All government data in digital format must be classified into the following categories: public or open data, confidential/sensitive data, secret, and top secret.

15.2.6. Access to data should not expire, and all data classified as public or open must remain accessible.

15.2.7. The public will enjoy on-demand access to data stored in the cloud.

15.2.8. The private sector shall make data available for development purposes in accordance with applicable data protection legislation.

15.2.9. Regulations to promote digital inclusion must consider social obligations, including, but not limited to, providing free data for indigent persons and households.

15.3. Creating a Digital Trust Environment

Digital transformation involves digitizing many activities and processes that govern the daily lives of citizens. This shift highlights the extent to which modern economies have become dependent on digitization in finance, health, education, agriculture, transport, entertainment,

and many other sectors. The danger in this dependency is that failure or endangerment of systems supporting the digital environment may lead to significant disruptions in services and the lives of people.

Less technologically savvy citizens need encouragement to leverage available digital technologies to improve their quality of life, facilitating transactions and access to government and commercial services without the inconvenience of long-distance travel and financial strain. The government has the responsibility to create an environment that fosters confidence in using digital technologies and platforms for daily needs.

To encourage the use of digital technologies, applications, and online platforms, the government needs to drive the creation of a secure cyber and online environment. This effort will strengthen and expand technology adoption and the use of digital solutions and platforms to address citizen needs. Citizens should also be empowered to report data breaches and online bullying, confident that their complaints will be addressed.

Many downloadable applications and credit providers require citizens to grant access to their mobile data, including contacts, location, and credit information, often without a commitment to ensure that such data is not shared or sold to other parties. Data protection authorities need to monitor these practices to prevent the abuse of citizen data for financial gain without benefits accruing to the citizen.

Although South Africa has legislation (Cybercrimes Act, POPIA) and policies (NCPF) addressing cybercrimes and online-related crimes, challenges exist in preventing, investigating, and prosecuting these crimes due to a lack of human capacity and financial resources. Law enforcement authorities need properly trained personnel to investigate and prosecute cybercrimes. Information regulators need to be capacitated to receive, investigate, and act on reported cases of data breaches and abuses promptly.

Some policies and frameworks, like MISS and NCPF, are outdated and may not be relevant to the current technology-based and data-driven environment. Consideration should be given to reviewing these policies to ensure their relevance in a digitally transformed government and society.

Cybercrime is a borderless crime, easily executed from any location. Treaties and conventions have been developed to enable cooperation among countries in preventing,

fighting, and prosecuting cybercrime. It is important for South Africa to examine existing conventions and treaties on cybercrime prevention to determine the need to sign and ratify those in the best interests of the Republic.

Citizens and enterprises might be prone to abuses by service providers due to a lack of information or legal support in giving consent for what happens to their data or subscribing to cloud services. Consent requests and service level agreements often contain complex, long-winded legal clauses that are difficult to process and understand. Customers may not be fully informed about the implications of using a particular cloud service provider until they attempt to switch providers and face unexpected complexities and potential data quality compromises.

Consumers might be tempted to use affordable cloud providers until problems arise, revealing that those providers lack the required capacity and competencies. Cloud providers should be transparent about their credentials and provide detailed information, licenses, and certificates.

Policy Interventions

15.3.1. Data protection authorities shall be adequately resourced and capacitated to:

15.3.1.1. Investigate, charge, and prosecute, where applicable, individuals involved in data breaches as outlined in data security and privacy protection legislation and policies.

15.3.1.2. Conduct awareness campaigns to help citizens understand and assert their rights concerning their data, as well as know how and where to report data breaches and other abuses or violations as outlined in POPIA, the Cybercrimes Act, and any other related policies and legislation.

15.3.1.3. South African data security and data protection legislation and policies shall be reviewed and adapted, when necessary, to ensure they are responsive to emerging threats in the cyber environment.

15.3.1.4. Data protection authorities should conduct periodic assessments of privacy performances for government agencies, businesses, and online platforms, taking appropriate action where breaches are discovered.

15.3.1.5. The Minister shall ensure that the Cybersecurity Hub is adequately capacitated and strengthened to respond to threats and risks associated with digitization.

15.3.1.6. All digital technologies used by the government should incorporate cybersecurity-by-design principles, including warning systems to detect and inform clients of potential cybersecurity threats in their infrastructure. This approach should cover the entire lifecycle of data collection, processing, use, storage, mining, and destruction.

15.3.1.7. The government shall prioritize the signing and ratification of regional, continental, and global treaties and conventions that support collaboration in the pursuit and prosecution of cybercrimes. The signing of such treaties must be guided by national interest, as articulated in the Framework Document on South Africa's National Interest and its advancement in the Global Environment.

Policy proposals

15.3.2. The government and private sector shall take appropriate security measures and adhere to South African data protection laws and protocols in the provision of data and cloud services.

15.3.3. The government, along with data and cloud service providers, must ensure robust data and cloud security measures are in place to mitigate cyber-attacks and data privacy violations, including establishing the necessary protocols.

15.3.4. All public bodies responsible for the protection of personal and government data shall conduct awareness campaigns to educate the public on the protection of personal data, privacy, and security.

15.4. Cross-Border Data Transfers and Data Sovereignty

The free flow of data is an important catalyst for robust internet services and the global exchange and sharing of information and data. Many multinationals, based in South Africa and other countries, rely on an open cross-border data regime to be able to manage their businesses across different jurisdictions. Any restriction to such cross-border flows can have a negative impact on such businesses. South Africa is an investment destination for many multinationals that are supporting local economic growth and jobs required for sustainable livelihoods.

POPIA provides for legal requirements regarding cross-border transfers of personal data. It is, however, possible that the South African government might be approached by other countries and organisations that seek data-sharing arrangements in certain areas, such as health, environment, fauna and flora. Where such requests might be viewed positively, it is

important to have guidelines that would determine the modalities of entering into such data sharing agreements.

The principles that guide such agreements should therefore be the same to avoid arbitrary decisions and agreements that might compromise the security and sovereignty of South Africa and ultimately cause harm to those they are intended to benefit.

South Africa is also participating in various digital trade and investment initiatives. A clear government cross-border data regime is necessary to guide those involved in related engagements and negotiations. Initiatives such as the AfCFTA, Smart Africa Single African Digital Market initiative and Southern African Customs Union initiatives fall under such categories.

Finally, cross-border data transfers and sharing should be carried out in such a manner as to respect the security and sovereignty of South Africa.

Policy Interventions

15.4.1. The processing of data collected within the borders of South Africa shall comply with South African data protection and security laws and policies.

15.4.2. Government data that incorporates content pertaining to the protection and preservation of national security and sovereignty of the Republic shall be stored only in digital infrastructure located within the borders of South Africa.

15.4.3. The government shall pursue cross-border data transfers and sharing agreements that meet the following criteria:

15.4.3.1. Agreements must promote national interests, including socio-economic development, security, and sovereignty.

15.4.3.2. Agreements must comply with the data protection and data security laws and policies of South Africa.

15.4.3.3. Agreements should enhance mutually beneficial cooperation for all parties involved.

15.4.3.4. Agreements should give effect to the African Continental Free Trade Area (AfCFTA), Southern African Customs Union, Single Digital African Market, and AU and SADC protocols.

Policy proposal

15.4.4. The processing of national data, including cross-border data-sharing, shall comply with South African data protection and security laws and policies.

15.5. Skills and Capacity Development

Data requires both technological and human input to convert it into actionable insights that solve everyday problems, initiate evidence-based policies, and develop tradable digital goods and services. Technologies themselves need human input to provide the necessary support.

Creating a digital economy and enabling inclusive participation also requires the capabilities to exploit and convert data into tradable goods and services. Therefore, digital skills are indispensable to a data-driven and digital economy. Digital literacy and expertise should be fostered across all levels of society, extending beyond formal training and education.

If digital skills are crucial for fostering digital economic inclusion through employment and innovation, it is essential to formalize the inclusion of digital skills in school curricula. Ensuring that teachers are formally trained to teach various digital skills and continuing to donate computer equipment to schools in disadvantaged areas can significantly impact the creation and expansion of an inclusive digital skills pool.

In South Africa, many organizations and institutions are involved in digital skills development initiatives, some of which are related to BBBEE compliance requirements. Existing research, such as the 2022 JCSE-IITPSA ICT Skills Survey, 12th Edition, largely indicates that these interventions do not have the necessary impact to bridge the digital skills gaps. The ideal solution is to coordinate all stakeholders involved in digital skills initiatives to ensure focused interventions and targets supported by monitoring and evaluation to maintain alignment with agreed goals and targets.

There are also global partners, including international organizations and other countries, that sponsor skills and capacity development initiatives both locally and online. It is necessary to identify potential beneficiaries from certain groups who would not ordinarily have access to such opportunities and provide them with the necessary support to enable their participation in these digital skills development initiatives.

Policy Interventions

15.5.1. The government shall develop an adaptable strategy for skills development and retention that aligns with changes in the digital and technology environment.

15.5.2. School syllabi should incorporate digital literacy and technologies across the learning ecosystem. The government will ensure that funding is made available for the resources required to implement this initiative effectively.

15.5.3. The Media, Information and Communication Technologies Sector Education and Training Authority (MICT-SETA) must consistently conduct skills surveys in the sector. This will help align skills development interventions with industry skills requirements, ensuring that the training provided meets current and future needs.

15.5.4. The National School of Government and other identified partners should develop and adapt digital skills programs to ensure the adoption and usage of digital technology across government.

15.5.5. Memoranda of Understanding entered with international partners regarding digital skills interventions shall prioritize unemployed youth and graduates, women, and people with disabilities.

15.5.6. The Minister shall support only those Equity Equivalent Investment Programmes skills interventions that are accredited and prioritize youth, unemployed graduates, startups, SMMEs, rural women, and youth.

Policy Proposals

15.5.7. The government and private sector shall ensure the provision of skills and capacity development programs to equip individuals and organizations with the necessary knowledge and expertise to leverage cloud-based technologies and applications.

15.5.8. The private sector is encouraged to support and provide advisory and technical assistance, including best practices, training, and technical support.

.

15.6. Competition in the Data and Cloud Market

The South African cloud and data centre business environment is predominantly dominated by multinational companies. This domination is largely due to the economies of scale that these companies have established over time. Competition issues arise when market concentration is structured in a way that deliberately bars new entrants. Additional

competition concerns can occur when there is deliberate collusion to exclude other competitors and new entrants.

Competition issues in the digital environment are particularly complex because companies can have a footprint in multiple jurisdictions without a physical presence. Therefore, further research is necessary to understand potential anti-competitive practices in the data and cloud market. Adequate capacity must be created to investigate these practices and implement appropriate measures to combat anti-competitive behaviour.

South Africa has a competition regulator, the Competition Commission, which has the capacity and competence to regulate competition issues in every sector. The Competition Commission has already undertaken merger and acquisition activity in the data centre market and initiated market inquiries to examine competition issues in digital markets. They have also implemented censures where anti-competitive behaviour by e-commerce and digital platforms was found to transgress competition rules. Thus, there is no empirical evidence necessitating a digital regulator focused solely on competition issues in the digital space.

Policy Interventions

15.6.1. The Competition Commission shall consider reviewing and potentially augmenting the Competition Act in relation to the data and cloud market, where empirical evidence indicates that the current law is inadequate to address competition issues in these markets.

15.6.2. 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.

15.6.3. 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.

15.6.4. Competition among data and cloud service providers shall be encouraged to foster competitive and innovative offerings, as well as to potentially reduce costs for consumers.

15.6.5. 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.

Policy proposal

15.6.6. Government must encourage more investment in data centre and cloud services.

15.7. Research and Development (R & D)

The Statists 2024 report shows that countries with the highest spending in research and development are the United States of America, followed by China, Japan, Germany and South Korea. It is therefore no surprise that all these countries are in the top 10 of the most technologically advanced countries.

South Africa increased its R & D spend during COVID-19, which likely explains the reason it was able to manage the pandemic much better than many countries, because its interventions were research-based.

In the digital environment, research is not only important for innovation and the development of new products and services, but also in identifying the digital innovations, new digital products and services that can be leveraged to advance the country's competitiveness and promote and reinforce localisation.

Concern expressed during engagement with StatsSA was that there are duplications in the research environment among government funded institutions and even private sector organisations, which not only lead to misaligned reporting, but also the duplication and wastage of resources. This indicates that in addition to funding R & D, it is also important to streamline South African research institutions to strengthen research capabilities, optimise scarce resources and encourage innovation and technology development.

Research capacity exists in government and government agencies, academia and independent research institutions. To support the digital economy, there is a need for collaboration and streamlining across all the research institutions to eliminate possible duplications that waste scarce resources necessary to support and strengthen technological development and innovation in South Africa. This alignment will therefore help to have focused research on digital technologies and innovations that can inform how South Africa can leverage data and cloud services to build and sustain a robust digital economy.

Policy Interventions

15.7.1. 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 with the business model for data and cloud research as articulated in the White Paper on Science, Technology, and Innovation.

15.7.2. The government shall increase R&D spending with a focus on supporting innovation and technology development. Additionally, the Technology Innovation Agency shall be adequately funded and capacitated to support South African innovators.

15.7.3. Academia, research institutions, industry, and innovation hubs must collaborate with the government in R&D, exploiting new technologies to build world-class data centres and cloud capabilities.

Policy proposal

15.7.4. South Africa must continue to encourage investment in R & D.

15.8. Governance and Institutional Mechanisms

Data governance refers to the exercise of authority, control, and shared decision-making, including planning, monitoring, and enforcement, over the management of data assets within one organization or across different organizations that share common data assets (OECD, 2019).

A data governance model must support existing and new processes to ensure the proper management, protection, production, and usage of data throughout its life cycle. This requires a collaborative and unified approach to managing valuable data assets. In this regard, developing a framework of ethical guidelines is crucial to eliminate biases associated with digital technologies. Additionally, the digital transformation of society and its resulting digital economy bring the emergence of various digital technologies which, if not properly monitored, could pose threats to the security and privacy of individuals.

Although establishing a single regulator for developing conformance standards for digital technologies might not be feasible due to the diversity and sectoral spread of these

technologies, empowering regulators in different sectors to develop regulatory regimes for these technologies is necessary.

Data-sharing and interoperability of systems are vital for supporting innovation and trading in digital goods and services, both locally and internationally. They also facilitate integrated planning and knowledge sharing across different sectors, including within and between levels of government, government departments, government and industry, and government and other stakeholders.

The government needs to find a balanced approach between security, constitutional, and legal obligations on one side, and encouraging and supporting innovation on the other. This requires systematic collaboration between government, industry, academia, non-governmental organizations (NGOs), and other civil society groups. Such collaborative efforts are necessary to ensure the sustainable growth and development of an inclusive digital economy and a digitally transformed society.

Policy Interventions

15.8.1. The Minister shall establish the Advisory Council consisting of the private and public representatives to, amongst others:

15.8.1.1 Ensure coordination and collaboration of the different initiatives and investments in data centres and cloud technologies.

15.8.1.2 Enhance data management standards, guidelines, best practices and the use of data for innovation and economic activities.

15.8.1.3 Provide technical support and assistance, including awareness programmes.

15.8.1.4 Provide input in the development of a regulatory framework for the management of data and cloud services.

15.8.1.5 Strategic data sets that can stimulate innovation, the economy and support service delivery.

15.8.1.6 Development of an Interoperability framework between government and other key stakeholders.

15.8.1.7 Any other matter relevant to the implementation or review of this Policy

15.8.2. 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.

15.8.3. 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.

15.8.4. 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.

Policy Proposal

15.8.5. Government and relevant regulators must develop specific regulatory frameworks, guidelines, norms and standards in support of this policy.

16. REVIEW OF THE POLICY

The National Data and Cloud Policy shall be approved by Cabinet.

The review of the National Data and Cloud Policy will be based on new developments in the ICT Sector and evolving digital environment.

17. IMPLEMENTATION APPROACH

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

As indicated in the policy interventions, structures comprising different professionals will be established to advise on the development of frameworks necessary to support the policy's implementation. These structures will include, but are not limited to, the following:

17.1 The Data Advisory Council consisting of private and public representatives including academia to advise the Minister amongst others, on data management standards, guidelines, best practices and the use of data for innovation and economic activities.

17.2 The Data and Cloud Technical implementation Task team comprising key government stakeholders such as DCDT, the SSA, Treasury, DPSA and Home Affairs. Other key stakeholders including National Treasury, Information Regulator, Statistics South Africa, Council for Scientific and Industrial Research (CSIR) and Competition Commission, may be brought on board to advise on specific matters. Other stakeholders may also be considered for participation owing to additional support areas that are identified during implementation.

18. KEY STAKEHOLDER ENGAGEMENTS

A diverse range of stakeholders was engaged to ensure that this policy reflects the perspectives and needs of different groups and to build broad-based support for its implementation. Amongst others, the stakeholders consulted in the development of this policy include government departments, industry experts, private sector representatives, and other stakeholders who may be affected by or have a vested interest in the policy.

The policy was finalised with engagement and input in from the following stakeholders:

18.1 Government Departments
18.2 Organs of the State responsible for security
18.3 Relevant national regulators
18.4 State Information Technology Agency (SITA)
18.5 Government Information Technology Officers Council (GITOC)
18.6 Industry organisations

19. CONCLUSION

The Data and Cloud Policy is a crucial lever to enable a digitally transformed South Africa, fostering a robust Digital Economy where all citizens have equitable opportunities to participate. This policy emphasizes key enablers such as affordable access to broadband services and digital devices, access to non-sensitive data, skills and capacity development, and research and development. It also reinforces governance requirements, including data privacy and security, consumer protection, cross-border transfers compliance, competition, and governance and institutional mechanisms.

This policy seeks to align with the African Union's goal of harmonizing data-related policies to enable safe and secure digital economic collaborations across the African continent and with other identified partners outside the continent. It recognizes that South Africa is part of the connected global community and cannot pursue its socio-economic goals in isolation.

Moreover, the policy is vital for improving the capacity and organization of the State to deliver services to all citizens by making government services accessible online. This ensures that old, indigent and persons with disability can access government services regardless of their location, whether rural, township, or urban. It also promotes access to non-sensitive processed government data, enabling innovation in digitally tradable goods and services. The

policy promotes connectivity and affordable, and free access to essential online services and government websites to ensure broad access to government services.

While the policy is not solely about data governance or security—since existing policies and legislation like POPIA, the Cybersecurity Policy Framework, and the Cybercrimes Act already cover these areas—it seeks to reinforce these policies. The primary goal is to enable South Africans to derive socio-economic value from data, driving innovation, inclusivity, and economic growth in a digitally empowered society.

20. REFERENCES

20.1 Government Legislation & Policy Guidelines

- Framework Document on South Africa's National Interest and its advancement in a Global Environment. 2023. [Available] https://www.dirco.gov.za/wp-content/uploads/2023/01/sa_national_interest.pdf
- Minimum Information Security Standards (MISS), 1996. [Available] https://www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20(MISS).pdf
- Minimum Information Interoperability Standards (MIOS) FRAMEWORK For Government Information Systems, 2017. [Available] https://www.sita.co.za/sites/default/files/documents/MIOS/Searchable%20-%20MIOS%20Framework%20V6%200.pdf
- National Archives and Record Service of South Africa Act (Act 43 of 1996). [Available] https://www.gov.za/documents/national-archives-south-africa-act
- National e-Government Strategy and Roadmap (Notice 886 of 2017). [Available] https://www.gov.za/sites/default/files/gcis_document/201711/41241gen886.pdf
- National Integrated ICT Policy White Paper (2016). [Available] https://www.gov.za/sites/default/files/gcis_document/201610/40325gon1212.pdf
- Promotion of Access to Personal Information Act (Act 2 of 2000). [Available] https://www.gov.za/documents/promotion-access-information-act#:~:text=The%20Promotion%20of%20Access%20to,provide%20for%20matters%20connected%20theretith.
- Protection of Personal Information Act (Act No. 4 of 2013) (POPIA). [Available] https://www.gov.za/documents/protection-personal-information-act
- Public Service IT Policy Framework (2001). [Available]

https://www.gov.za/sites/default/files/gcis_document/201409/it0.pdf

- Public Service Regulations, 2001. [Available] https://www.dpsa.gov.za/dpsa2g/documents/acts&regulations/regulations1999/PSRegulations_13_07_2012.pdf
- DPSA determination and directive on the usage of cloud computing services in the public service. [Available] https://www.dpsa.gov.za/dpsa2g/documents/egov/2022/egovernment_02_02_2022.pdf

20.2 International Data And Cloud Standards

- Cloud Watch (EU) D4.1 – Cloud certification guidelines and recommendations. [Available] https://docplayer.net/10806296-D4-1-cloud-certification-guidelines-and-recommendations.html
- Code of Practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services. [Available] https://www.isomanager.com/iso-27017-code-of-practice-iso-27002-information-security-controls-for-cloud-security.html
- ITU Big data – Cloud computing-based requirements and capabilities (Y 3600, 11/2015). [Available] https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-RECY.3600-201511-I!!PDF-E&type=items
- ITU Cloud computing – Framework and high-level requirements (Y 3501, 06/2016). [Available] https://www.itu.int/dms_pubrec/itu-t/rec/y/T-REC-Y.3501-201606-I!!TOC-HTM-E.htm
- ITU cloud computing 'Joint Coordination Activity' (Document 180, Period 2013 – 2016). [Available] https://www.itu.int/en/ITU-T/jca/idm/Documents/docs-2012/JCAIDM-136-R1.docx
- ITU Guidelines for cloud service customer data security (x 1641, 09/2016). [Available https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-X.1641-201609-I!!PDF-E&type=items
- ITU Information Technology – Cloud computing – Reference architecture (y 3502, 08/2014). [Available] https://www.itu.int/dms_pubrec/itu-t/rec/y/T-REC-Y.3502-201408-I!!SUM-HTM-E.htm

- ITU Overview of end-to-end cloud computing management (Y.3521/M.3070, 03/2016). [Available]https://www.itu.int/rec/T-REC-Y.3521-201603-I
- ITU Security Framework for Cloud Computing (X.1601, 01/2014). [Available]
- https://www.itu.int/rec/T-REC-X.1601/en
- ITU's ISO/IEC 27001, dealing with Information Technology, Security techniques, Information security management systems Requirements. [Available]
- https://pecb.com/whitepaper/iso-27001-information-technology--security-techniques-information-security--management-systems---requirements

20.3 Articles by Experts

- Abell, T, Husar, A & Lim, MA. 2021. *Cloud computing is a key enabler for digital government across Asia and the Pacific*. Asia Development Bank (ADB) Sustainable Development working paper series no. 77. [Available] https://www.adb.org/sites/default/files/publication/707786/sdwp-077-cloud-computing-digital-government.pdf
- Amin, R. & Edward, H. 2022. *Government Migration to Cloud Ecosystems: Multiple Options, Significant Benefits, Manageable Risks.* [Available] https://www.worldbank.org/en/events/2022/06/12/government-migration-to-cloud-ecosystems-wbg
- Bali, A. 2019. *How AI Uncovers the Human Profiles in Your Cluttered Data*. [Available] https://bluexp.netapp.com/blog/how-ai-shapes-data-management-and-compliance-part-3
- Brooks, T, Robinson, J & McKnight, L. 2012. Conceptualizing a Secure Wireless Cloud. *International Journal of Cloud Computing and Services Science* 1 (3): 89- 114.
- Eggers, WD & Bellman, J. 2015. *The journey to government's digital transformation*. [Available] https://www2.deloitte.com/content/dam/insights/us/articles/digital-transformation-in-government-summary/DUP_1424_Journey-to-govt-digital-future_EXEC-SUMMARY.pdf
- Govindaraj, P & Jaisankar, N. 2017. A Review on Various Trust Models in Cloud Environment. *Journal of Engineering Science and Technology Review* 10(2):213-219
- ITU 2019. Digital transformation and the role of enterprise architecture [Available] https://www.itu.int/pub/D-STR-DIG_TRANSF-2019
- ITU. 2012. *Cloud Computing in Africa: Situational Analysis & Perspective.* [Available]

https://www.itu.int/ITU-D/treg/publications/Cloud_Computing_Afrique-e.pdf

- Kugler, K. 2022. The Impact of Localisation Laws on Trade in Africa. POLICY BRIEF 08. Mandela Institute. [Available] https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-lawandmanagement/researchentities/mandelainstitute/documents/researchpublications/PB%2008%20Data%20localisation%20laws%20and%20trade.pdf
- Liang, S & Ulander, P. 2021. *7 Requirements for Building Your Cloud Infrastructure.* [Available]https://www.cio.com/article/282625/cloud-computing-7-requirements-for-building-your-cloud-infrastructure.html
- Nichols, K & Sprague, K. 2012. *How Government Can Get Ahead in Cloud* [Available] https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/BTO/PDF/MoB25_Cloud_MoG.aspx
- Nyamwena, J & Mondliwa, P. 2020. *Data Governance Matters: Lessons for Southern Africa*. [Available] https://www.competition.org.za/ccred-blog-digital-industrialpolicy/2020/7/28/data-governance-matters-lessons-for-south-africa
- OECD (2021), "SMEs in the online platform economy", in *The Digital Transformation of SMEs*. [Available] https://doi.org/10.1787/1386638a-en
- OECD 2014. *The Concept, Impacts and the Role of Government Policy*. [Available] https://www.oecd-ilibrary.org/science-and-technology/cloud-computingthe-concept-impacts-and-the-role-of-government-policy_5jxzf4lcc7f5-en
- OECD. 2019. *Enhancing Access and Connectivity to Harness Digital Transformation*. [Available] https://www.oecd.org/sti/broadband/enhancing-access-digital-transformation.pdf
- OECD. 2021. The Digital Transformation of SMEs. [Available] https://www.oecd.org/publications/the-digital-transformation-of-smes-bdb9256a-en.htm
- Pokharel, M. 2014. *The Future of Data for e-Governance* [Available] https://www.researchgate.net/publication/224128375_The_future_data_center_for_-governance/citation/download
- SITA. 2020. Value Proposition of Cloud Computing and the Government Private Cloud Ecosystem (GPCE) Report.
- State Of Public Cloud Migration, 2020, a commissioned study conducted by Forrester Consulting on behalf of Google, May 2020. [Available]

https://services.google.com/fh/files/misc/googlecloudmigrationsnapshotreportfinal2022.pdf?hl=ja

- United Nations Conference on Trade and Development (UNCTAD). 2022. Data and Digitalization for Development: Outcome report. eCommerce week 25-29 April 2022. [Available] https://unctad.org/system/files/information-document/eWeek-2022Outcome-Report-FINAL1.pdf
- World Bank. 2018. *South Africa Digital Economy Assessment*. [Available] http://hdl.handle.net/10986/33632

21. DEFINITIONS

"Acquisition" means a hostile or unfriendly takeover deal, in which the target company does not wish to be purchased.

"Broad network access" means resources hosted in a private cloud network (operated within a company's firewall) that are available for access from a wide range of devices such as tablets, PCs, Macs and smartphones.

"Cloud computing" is defined and described by the ITU Study Group 1 as having the following key characteristics:

- Broad network access.
- Measured service.
- Multi-tenancy.
- On-demand self-service.
- Rapid elasticity and scalability; and
- Resource pooling.

"Cloud infrastructure" means hardware and software components – such as servers, storage, networks and virtualisation software – that are needed to support the computing requirements of a cloud computing model.

''Constitution'' means the Constitution of the Republic of South Africa, Act No. 108 of 1996.

"**Cybersecurity**" is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets.

"**Cybersecurity Hub**" means a Computer Security Incident Response Team established to pool public and private sector threat information for processing and disseminating such information to relevant stakeholders.

"**Data**" refers to electronic representation of information in any form.

"**Data analytics**" refers to utilising data, machine learning, statistical analysis and computer-based models to get better insight and make better decisions from data.

"Data centres" means centralised locations where computing and networking equipment is concentrated to collect, store, processing, and distributing or allowing access to large amounts of data.

"Data classification" refers to a process of organising data by relevant categories so that it may be used and protected more efficiently.

"**Data controller**" refers to an individual or organisation that manages how data is processed and is responsible for complying with data protection regulations.

"Data embassies" refer to a solution traditionally implemented by nation-states to ensure a country's digital continuity with respect to critical databases, where such databases are in another country while remaining within the country's jurisdiction.

"Data operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

"Data portability" means the right of the data subject to obtain data that a data controller holds on them, and such data is in a structured, commonly used and machine-readable format, and to re-use it for their own purposes.

"**Data sharing**" refers to sharing the same data resource with multiple applications or users.

"**Data subject**" refers to an identifiable living person to whom a particular data item relates.

"Devices" refers to electronic equipment adapted to perform a particular function.

"Digital economy" means a hyper-connected economy characterised by a growing number of interconnected people, organisations and machines through the web and using digital technologies which includes advanced manufacturing, robotics and factory automation, new sources of data from mobile and ubiquitous internet connectivity, cloud computing, big data analytics and artificial intelligence.

"**Digital infrastructure**" means joint fibre-optic and wireless-based advanced ICT platforms with embedded multi-functional application services that facilitate 24/7 online real-time connectivity between nodes in the operational network to allow remote management of production assets.

"**Digital skills**" in the context of this policy refer to a range of abilities to use digital devices, communication applications, and networks to access and manage information.

"**Digital technologies**" are electronic tools, systems, devices and resources that generate, store or process data.

"Digital transformation" is a continuous process of multi-model adoption of digital technologies to fundamentally change the way services are ideated, planned, designed, deployed and operated such that they are personalised, paperless, cashless, frictionless and consent based.

"Digital trust" is the confidence users have in the ability of people, technology and processes to create a secure digital world (i.e. provide safety, privacy, security, reliability, and data ethics with their online programs or devices).

"Digitalisation'' 'is the process of leveraging or using digitised information to improve business processes.

"Digitisation" is the process of converting information from a physical or analogue format to a digital format.

Government Data is all stored data of the public sector which could be made accessible by government in a public interest without any restrictions for usage and distribution.

''Minister'' means the Minister of Communications and Digital Technologies.

"Multi-tenancy" means the mode of operation of software where multiple independent instances of one or multiple applications operate in a shared environment. The instances (tenants) are logically isolated but physically integrated.

"**National critical information infrastructure**" means all ICT systems, data systems, databases and networks (including people, buildings, facilities and processes), that are fundamental to the effective operation of the Republic of South Africa.

"**Non-sensitive data**" means data that is already a matter of public record or knowledge. In South Africa, access to such data/information is enabled through PAIA.

"On-demand self-service" means that a consumer can request and receive access to a service offering, without an administrator or support staff having to fulfil the request manually.

"Open data" means data that is made freely available to everyone for use, re-use and republishing as they wish, subject to ensuring the protection of privacy, confidentiality and security in line with the Constitution.

"**Confidential, Secret & Top Secret Data**" as defined in the Minimum Information Security Standards.

"**Sensitive data**" means data that must be protected from unauthorised access to safeguard the privacy or security of an individual or organisation.

''**Personal information''** refers to personal information as defined in POPIA.

"**Public Cloud**" is a platform that uses the standard cloud computing model to make resources -- such as virtual machines, applications or storage -- available to users remotely. Public cloud services may be free or offered through a variety of subscription or on-demand pricing schemes, including a pay-per-usage model.

"**Private cloud**" is a cloud platform in which all hardware and software resources are dedicated exclusively to, and accessible only by, select users or a single customer.

"Public data" in the context of this policy means all information and data held by the government and its entities that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage.

"Re-use and redistribution" mean that the data must be provided under terms that permit re-use and redistribution including intermixing with other datasets.

"**Sensitive data**" means data that must be protected from unauthorised access to safeguard the security of a national asset, the privacy or security of an individual or organisation by Chapter 4 of the PAIA (Act 2 of 2000).

"Software" refers to a set of instructions, data or programmes used to operate computers (and similar equipment) and execute specific tasks.

"Special Economic Zones (SEZs)" means geographically designated areas within South Africa, set aside for specifically targeted economic activities to promote national economic growth and export by using support measures to attract foreign and domestic investment and technology.

"Submarine communications cable" means a cable laid on the seabed between land-based stations to carry telecommunication signals across stretches of ocean and sea.

"Systems interoperability" means the ability of systems and services that create, exchange and consume data to have clear, shared expectations for the contents, context and meaning of that data.

"**Zettabyte**" refers to a unit of information equal to one (1) sextillion bytes (1,000,000,000,000,000,000,000).