Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID AFRIKA

Vol. 670 1 April / April 2021 No. 44389

ISSN 1682-5845

9 771682 584003 44389

Contents

GOVERNMENT NOTICES • GOEWERMENTSKENNISGEWINGS

DEPARTMENT OF COMMUNICATIONS AND DIGITAL TECHNOLOGIES

NO. 306 **1 April 2021**

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

INVITATION TO SUBMIT WRITTEN SUBMISSIONS ON THE PROPOSED NATIONAL DATA AND CLOUD POLICY

1.1 The Minister of Communications and Digital Technologies hereby publish the proposed National Data and Cloud Policy in terms of section 3(5) of the Electronic Communications Act, 2005 (Act No. 36 of 2005), for comment.

1.2 Interested persons are invited to submit written submissions in relation to the proposed policy within 30 working days of the date of publication using the following options:
1.) Written comments addressed to the following contact details

The Director-General, Department of Communications and Digital Technologies For attention: Ms. C Lesufi, Director, Telecommunications Policy
First Floor, Block A3, iParioli Office Park, 1166 Park Street, Hatfield, Pretoria
Private Bag X860, Pretoria, 0001
DataCloudpolicy@dtps.gov.za; Tel: 076 529 7374

or 2.) Complete online at the following link: https://forms.office.com/r/mTc6cBvgfh

or 3.) Scan this QR code to access online submission form from your smartphone

Comments received after the closing date may be disregarded.

Ms Stella Ndabeni-Abrahams, MP
Minister of Communications and Digital Technologies

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

DRAFT NATIONAL POLICY ON DATA AND CLOUD

Draft National Policy on Data and Cloud

Table of Contents

1. Background and Context

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 model, shifting them towards digital domains, ensuring that citizens and customers can access the services securely at any given time, anywhere and through any device.

The digital domain is increasingly becoming a critical element for delivering efficiencies in the economy. Trade across borders is increasingly being facilitated by the internet and e-commerce platforms. Digital platforms create scalable implementations through the large-scale ecosystems which they enable. Collaboration with other ecosystem partners is easily orchestrated by digital platforms.

In their first draft recommendation report on Open Science, the United Nations Educational, Scientific and Cultural Organization (UNESCO) (2020) emphasised that for countries to realise the full benefits of the digital economy, there is a need to accelerate investment in broadband infrastructure, and increase investment in digital infrastructure and associated systems.

The South African economy is characterised by low economic growth, increasing levels of poverty, poor education, low skills and high levels of unemployment. The emergence of the COVID-19 pandemic has heightened the social and economic challenges that the country is facing. However, the advent of the Fourth Industrial Revolution (4IR) and its related technologies presents an opportunity to address the social and economic challenges characterising the South African economy.

South Africa's effective response to these challenges will depend significantly on the extent to which it exploits opportunities presented by the digital economy, through the development of policy frameworks that harness the economic and social potential of data and cloud computing. Such policy frameworks should be citizen-centric and support already existing government initiatives of universal access and affordability of services. Most importantly the frameworks should ensure that challenges associated with lack of access to digital infrastructure, devices, software, applications and digital skills are addressed. Access to reliable, affordable digital infrastructure and required skills is critical to enable the digital economy.

4

One of the greatest advantages of data is the value it generates after it is processed into information and knowledge. However, it is also well recognised that the capacity to use and transform data into information and knowledge lies in the hands of mega technological digital companies, which are highly operational in selected countries. Data facilitates communication between machines, smart devices, and individuals, as well as transactions between businesses and customers, government and its citizens and government and businesses. It is, therefore, essential that South Africa develops its own indigenous capacity.

According to the global Digital Evolution Index (Chakravorti, B & Chaturvedi, RS, 2017), when it comes to network readiness for the digital economy, South Africa is in close proximity to Thailand and slightly ahead of Brazil, Indonesia and Morocco among others.

There is a need to recognise that data is the infrastructure for the digital economy and therefore the driver behind 4IR and the enabler of macro-economic development. It requires acceleration to drive a rapid rate of digital economic development.

There are huge numbers of data sets generated daily through various services and transactions. Government generates, collects and stores huge volumes of data through the services it provides to the general public. The private sector conducts, collects and generates extremely large volumes of data through various services and business transactions. Similarly, academic institutions generate and collect extremely large volumes of data as a result of research. It is projected that by 2025, the global data sphere will grow to 163 zettabytes (a trillion gigabytes) from 40 zettabytes in 2019. Storage and management of these enormous amounts of data are made possible by cloud computing.

The digital domain is increasingly becoming a critical component in delivering efficiencies in the economy. Trade across borders is increasingly being facilitated by the internet and ecommerce platform. Digital platforms create scalable implementations through large-scale ecosystems which enable collaboration with other ecosystem partners and are easily orchestrated by the digital platforms.

Recognising that the expansion of the digital economy is characterised by the uptake and use of various 4IR technologies, it is clear that the adoption of strategies and interventions to exploit opportunities presented by data and cloud computing will enable the development of various applications, services and technologies. The development of applications, services and solutions will address challenges of service delivery and economic inclusion, and will enable South Africa to become globally competitive.

The digital economy is a sharing economy where many enterprises and other actors in the economy are able to leverage digital platforms horizontally for commercial and social gain. Digital platforms, through their scalability to higher economies of scale, deliver a near zero marginal cost economy, meaning that once the platform has been developed and deployed, the incremental cost of placing additional users onto the platform are almost negligible. This is an important characteristic of the digital economy, especially in developing economies where significant inequalities and dichotomies exist in the economy.

For countries to realise the full benefits of the digital economy, there is a need to accelerate investment in broadband infrastructure, and increase investment in data centre infrastructure and associated systems such as cloud computing capacity. Investment in infrastructure needs to be supported by clear protocols for information technology security, cyber security and a data governance framework supporting open data principles.

The envisaged overall policy framework on data and cloud must be biased towards open standards and open systems, including open source frameworks rather than closed and exclusive systems. The integrity of any digital economy, as a sharing economy, depends on the extent to which it delivers the sharing advantages to its ecosystem partners, and its ability to drive openness whilst protecting citizens, customers and partners.

2. Policy, Legislative and Regulatory Landscape

South Africa's various policies, legislation and regulations, initiated shortly after 1994, did not sufficiently appreciate the reality of data in the digital economy. The Electronics Communications and Transaction Act (ECTA), Act No. 25 of 2002; Electronic Communication Act (ECA), Act No. 35 of 2005; Independent Communications Authority of South Africa (ICASA) Act, Act No. 13 of 2000; and Competition Commission Act, Act No. 89 of 1998, were established when internet usage was significantly low in relation to the population of South Africa. In 1998 internet usage was estimated at 2.3% of the population; in 2003, 6.3%; in 2008, 9.9%; and in 2012, 28.3% (BMI-T, 2013). The most recent data (World Bank, 2017) estimated that 56% of the population had internet access in 2017. In the early years the emphasis was on voice communication via mobile and telephone, while today communication (including business transactions, government interactions with citizens, and interaction between machines) is largely data intensive and internet driven (Ngcaba, 2020). Today, there is rapid and dynamic convergence of technology domains (cyber, physical, and biological) and intelligent digital technologies are deployed beyond telecommunications and postal

services. The wide deployment of intelligent digital technologies is beyond the regulatory scope of the existing regulatory authorities.

More recent policies do recognise a data-intensive and data-driven economy, and the associated risks. The White Papers on STI (2019) and National Integrated ICT (2017) emphasise the need for open data. The 2017 National e-Government Strategy and Roadmaps advocate service delivery and interactions with citizens over digital platforms and ecosystems. The Protection of Personal Information Act, Act No.4 of 2013, which established the Information Regulator, recognises the need to protect the personal information of South Africans within and across the border. On the mandate that 'All People in South Africa are free and safe', the Justice, Crime Prevention and Security (JCPS) cluster issued the 2015 National Cybersecurity Policy Framework (NCPF), in response to cyberspace as the new crime scene and battlefield.

Data, including that generated by government, is largely stored in privately owned data bases. Despite South Africa's recent policy, legislative and regulatory responses to a data intensive and driven economy, there is no policy to guide localised data acquisition, ownership, storage, use and analytics. This is a threat to both national security and social and economic growth. A 2020 report by the Presidential Commission on 4IR recommends that South Africa 'Secures and avails data to enable innovation' (DCDT, 2020). The innovation includes service delivery, which is reimagined under the 'District Development Model.'

The current legal, policy and regulatory regimes create mandates administered by different government departments, with no coordination to support and drive the development of the digital economy. It is evident that when these policies, legislation and regulations are looked at collectively, they do not adequately address the ideal policy and regulatory environment. Some of these are listed in the table below.

Electronic Communications and Transaction Act, Act No. 25 of 2002 (ECTA)	Provides for identification, protection and management of critical data and critical databases. It further provides that these databases should be declared by the Minister as being for the protection of national security or economic and social wellbeing of the country.
Minimum Information Security Standards, 1996 (MISS)	Provides standards for the minimum information security measures that any institution must put in place for sensitive or classified information to protect national security.
Protection of Personal Information Act, Act No. 2013 (POPIA)	Provides for the protection of personal information against unauthorised use and access. The Information Regulator regulates the flow of personal information inside and outside the borders of South Africa and ensures access to information.

Protection of Information Act, Act No. 84 of 1982	Provides for the protection from disclosure of certain State information.
Public Administration Management Act, Act No. 11 of 2014	Provides norms and standards to ensure the inter-operability of its information systems for public administration and eliminates unnecessary duplication of information and communication.
National Archives of South Africa Act, Act No. 43 of 1996	Provides for the management of the electronic records system of government. It further provides for access to public records after the lapse of a 20-year period.
Spatial Data Infrastructure Act, Act No. 54 of 2003	Provides for the establishment of South African Spatial Data Infrastructure as the national technical, institutional and policy framework to facilitate the capture, management, maintenance, integration, distribution and use of spatial information.
Promotion of Access to Information Act, Act No. 2 of 2000 (PAIA)	Provides for access to any information including records held by public and private bodies.
National e-Strategy, 2017	Provides for innovative use of ICTs (including mobile devices, websites and other ICT applications and services) to link citizens and the public sector, with the aim of facilitating collaborative and efficient governance, improving the efficiency of government processes, strengthening public service delivery and enhancing participation of citizens in governance.
South African Cybersecurity Framework, 2012	Provides for a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure whilst strengthening shared human values and the understanding of cybersecurity in support of national security imperatives and the economy.
National Integrated ICT Policy White Paper, 2016	Provides for an open data policy framework with the following policy objectives: • Set out the principles that will inform the development of an open data action plan to allow everyone to access, use and re-use non-personal and unclassified public information and data. • Make non-personal and unclassified government-held data more widely available and usable, taking into account the South African legal context. • Promote informed, active citizenship by providing the framework to facilitate access to public data. • Promote innovation and economic growth by facilitating greater access to data which will enable entrepreneurs to better understand their communities and markets. • Promote efficiency and cost-effectiveness in the public sector by making it easier and less costly for government entities to access and re-use their own data and that of other public agencies. • Promote evidence-based policy making across government. The policy further emphasises commitment to ensure that key non-personal public information and data are freely available to everyone to use, re-use and republish as they wish, subject only to restrictions to protect privacy, confidentiality and security in line with the Constitution.

3. Rationale for the Data and Cloud Policy

The national agenda of government seeks to accelerate interventions aimed at unlocking investment opportunities, ensuring inclusive economic growth, and job creation. In this regard, the National Development Plan (NDP) provides for the need to intensify South Africa's global presence and competitive advantage; increase investment and grow the economy to create jobs that are sourced in domestic orientated businesses; and grow small-and medium-sized firms. Secondly, the vision of the NDP is to have universally accessible broadband connectivity that meets the needs of the country concerning cost, speed, and quality for all South Africans.

Thirdly, the NDP highlights the need for South Africa to sharpen its innovative edge and contribute to global scientific and technological advancement. Pursuant to this, the President established the Presidential Commission on 4IR to advise him, and government as a whole, on the development of a country strategy for South Africa on the 4IR. Following the conclusion of work by the commission, the Department of Communications and Digital Technologies (DCDT) has put in place mechanisms to give effect to the work of the commission by facilitating, coordinating and monitoring 4IR initiatives in South Africa.

The Data and Cloud Policy seeks to strengthen the capacity of the State to deliver services to its citizens, ensure informed policy development based on data analytics, as well as promote South Africa's data sovereignty and the security thereof.

4. Global Trends

The digital economy continues to grow exponentially, driven by cloud computing technologies that enable collection, analysis and synthesising of massive amounts of digital data. Data is a primary driver for the digital economy, whose massification is projected to reach 150,700 GB per second by 2022, underpinned by digital transformation and the Internet of Things (IoT) (United Nations Conference on Trade and Development [UNCTAD] Report, 2019).

According to the above UNCTAD Report, 70% of the digital data traffic is currently located in the Asia Pacific and North America regions, and these account for the highest percentage of the world's digital data. Going forward, the highest growth is forecast to occur in the Middle East and Africa at 41% per year, followed by the Asia Pacific at 32%.

The Domo's Data Never Sleeps 5.0 Report states that there are 2.5 quintillion bytes of data created each day. The study further states that the current pace is further accelerating with the growth of the IoT. However, the 2012 New IDC Digital Universe study states that only 0.5 % of the world's data generated is being analysed and used. It points out that this 0.5 % is shrinking as more data is generated and collected.

The exponential growth in data has created a need for more and dynamic storage solutions, which cannot be met by traditional computing systems. Cloud computing is seen as a platform to provide solutions to problems associated with the storage and management of the enormous amounts of data generated. Cloud computing is referred to as a large computational infrastructure to ensure successful data processing and analysis (Hashem, Yaqoob et al, 2014).

According to Bhardwaj et al, 2010, cloud computing services that would be ideal include the following:

- allows users access to a computing platform to develop a host of online applications. Infrastructure as a service (IAAS) – Infrastructure as a service gives users access to virtualised computing resources that can be scaled to their needs. This allows companies and governments to purchase computing resources on a metered basis, much the same as they would purchase electricity, water, and other utility services.
- Software as a service (SAAS) – Software as a service is how mist consumers today encounter cloud computing. Rather than run software locally on a personal computer they run the software in the cloud computing infrastructure.
- Platform as a service (PAAS) – Platform as a service

In recognising the importance of data for the digital economy, there is significant international movement towards the development of strategies and policies to fully exploit the opportunities presented by data and cloud computing. 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).

In addition, the data ecosystem brings with it the critical need for policy and legislation relating to the use of data, and to ethics and security. There is an emerging trend towards the development and enactment of policies and legislation that extend beyond basic laws on the

protection of personal data, e.g. Rwanda, Canada, India and Botswana, among others. This is being complemented by strategies, policies, resources, and legislation to exploit the benefits of the 4IR.

5. Purpose

This policy seeks to enable South Africans to realise the socio-economic value of data through the alignment of existing policies, legislation and regulations. The policy further seeks to put in place a conducive and enabling environment for the data ecosystem to thrive.

6. Scope

This policy is applicable to:

- All three levels of government (national, provincial and local);
- Organs of State/Public Enterprises;
- Private Sector; and
- General public/individual citizens.

7. Vision

Towards a data intensive and data-driven South Africa

8. Objectives

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

- Promote connectivity and access to data and cloud services;
- Remove regulatory barriers and enable competition;
- Ensure implementation of effective cybersecurity privacy, and data and cloud infrastructure protection measures;
- Provide for institutional mechanisms for the governance of data and cloud services;
- Support the development of small, medium, and micro enterprises (SMMEs); and
- Provide for research, innovation, and human capital development.

9. Definitions

"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.

"Data" means electronic representations of information in any form suitable for communication, interpretation, or processing by human beings or by automatic means.

"**Cybersecurity**" is the practice of making the networks that constitute cyberspace secure against intrusions; maintaining confidentiality, availability and integrity of information; detecting intrusions and incidents that do occur; and responding to and recovering from them.

"Cybercrime" means illegal acts, the commission of which involves the use of information and communication technologies.

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

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

"**Databank**" means a repository of information on one or more subjects that are organised in a manner that facilitates local or remote information retrieval and is able to process many continual queries over a long period of time.

"Data centres" means centralised locations where computing and networking equipment is concentrated for the purpose of collecting, storing, 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 concentration" means the concentration of significant quantities of data between a small number of firms, thus creating barriers for new entrants.

"Data exportability" means the automated or semi-automated transfer of data sets between different software applications.

"Data 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.

"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 Trust" is a legal structure that provides independent third-party stewardship of data for a defined purpose.

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

"Digital access" means the ability to fully participate in a digital society. It is about the equitable distribution of technology and online resources.

"Digital economy" means a hyper-connected economy characterised by a growing number of interconnected people, organisations and machines through the web and by the use of digital technology 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 evolution index**" is a data-driven holistic evaluation of the progress of the digital economies of 60 countries, using the following indicators:

1) Supply (internet access and infrastructure);
2) Consumer demand for digital technologies;
3) Institutional environment (government policies/laws and resources); and
4) Innovation (investments into R&D, Digital Start-ups etc.).

"**Digital infrastructure**" means joint fibre-optic and wireless-based advanced information and communication technology 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, and 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.

"Economic rights" refers to the rights to work in safe conditions, earn a wage that will provide for a minimum quality of living, organise or unionise, and access social security or protection where an individual is unable to work, as well as the right to freedom of trade, occupation and profession.

"First-mover advantage" means competitive advantage gained by being the first to bring in a new product category and being in control of resources relating thereto.

"Hyper-scale data centres" means large-scale data centres, often designed for a homogeneous scale-out Greenfield application portfolio using increasingly disaggregated, high-density and power-optimised infrastructures. They have a minimum of 5 000 servers.

"Metadata" means data that describes other data and processes. It is information and documentation which makes data understandable and sharable over time.

''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, networks (including people, buildings, facilities and processes), that are fundamental to the effective operation of the Republic of South Africa.

"Non-personal data" refers to data that does not contain personally identifiable information.

"**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 protection of privacy, confidentiality and security in line with the Constitution.

"Open data platform" is a digital platform that enables the access, use and sharing of data.

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

''**Personal information''** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

"Public data" in the context of this policy means all information and data held by government and its entities.

"Re-use and redistribution" means 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 privacy or security of an individual or organisation.

"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 sea bed between land-based stations to carry telecommunication signals across stretches of ocean and sea.

"**Zettabyte**" refers to a unit of information equal to sextillion (1000 000 000 000 000 000 000).

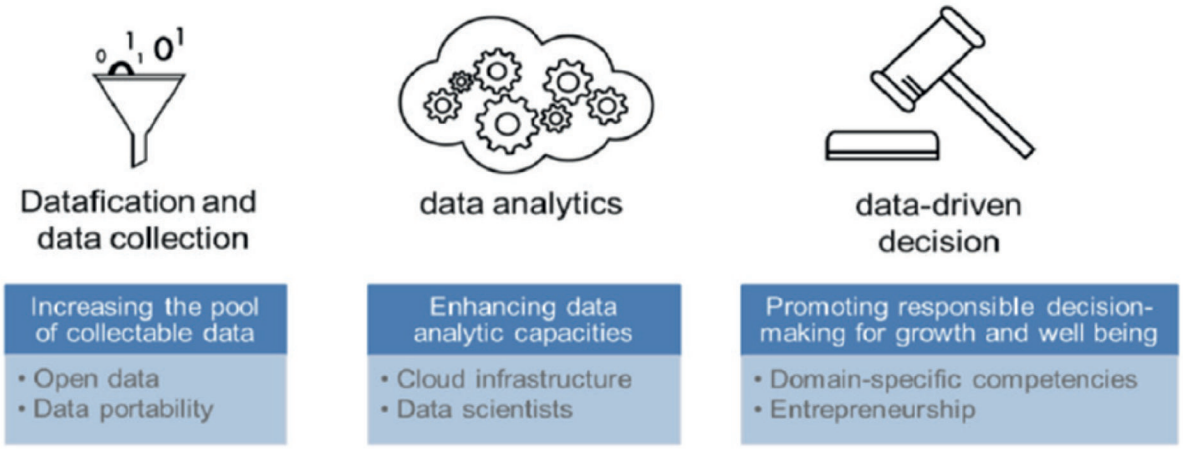
10. Policy Intent

The policy intent is aligned with the OECD Framework which links the data value cycle and policy issues shown in Figure 1. The cycle includes three components, namely datafication and data collection, data analytics, and data-driven decisions. To unlock the value of data, there are key policy issues that need to be addressed such as increasing the pool of collectable data, enhancing data analytic capacities, and promoting responsible decision making for growth and well-being, as depicted in Figure 1.

The policy is further informed by the following policy issues:

- Privacy;
- Competition and trade;
- Cybersecurity measures;
- Localisation and cross border data transfer;
- Governance and institutional mechanisms;
- Skills and capacity development;
- Research and innovation; and
- Human capacity development.

Figure 1: OECD framework which links data value cycle and policy issues



Source: Hill et al. (2015, p. 62).

10.1 Policy issues on Digital Infrastructure

Electronic communication networks and mobile communication networks constitute the cornerstone of the digital transformation of society. Universal access and service are critical to digital transformation. Without universal, secure electronic communication networks and mobile communication networks and connectivity, many of the promised benefits of digital

transformation may not be realised. The development of digital infrastructure has been one of government's priorities since the attainment of democracy.

The DCDT's 2017 National e-Government Strategy is transforming government's service delivery model towards significant utilisation of digital technologies. To fully obtain the benefit of the digital economy, it is important for government to review its own policies and the rules through which it acquires, uses, and engages with digital technologies. Digital platforms deliver economies of scale through architecture that enables various business entities and government entities to use a common platform.

At the heart of digital transformation is the development of an online identity for all citizens in support of service delivery and economic emancipation.

The National Integrated ICT Policy White Paper, 2016 recognised that South Africa remains a deeply unequal society and advocated, amongst other matters, for a Wireless Open Access Network (WOAN) to extend the digital infrastructure footprint and services. The policy also put in place measures to ensure rapid deployment of electronic communication infrastructure. It is against this background that the proposed policy intervention on digital infrastructure intends to bridge the digital gap, thus ensuring universal access to cloud and data infrastructure services for all South Africans. The proposed policy intervention cannot be viewed in isolation of other existing inclusion strategies such as South Africa Connect and the National Broadband Policy which seek to ensure that all South Africans have access to broadband services through well-defined targets by 2030.

Similarly, the 2019 Ministerial Policy on High Demand Spectrum and Policy Directions on the Licensing of a WOAN is intended to pave the way for the deployment of a nationwide 4G and ultimately 5G network in the South African mobile market.

In recognising these, to date South Africa has developed plans and policy interventions with well-defined targets to bridge the digital divide. What remains a challenge, however, is the slow pace of implementation and regular review of such plans and policy interventions.

The Presidential Commission on the 4IR recommends the importance of government tapping into the power of emerging digital infrastructure, technologies and innovation encapsulated

under the banner of the digital economy to advance a range of social and economic development priorities.

The Commission further recommends an ICT infrastructure framework that will support key economic sectors for digital development in South Africa with international connectivity, national connectivity, and data centres such as high computing and data processing and storage facilities, and last-mile broadband connectivity (mobile and fixed).

Given the centrality of digital infrastructure in the South African economy (since most services are delivered over such infrastructure), digital infrastructure of critical scale should be declared a national strategic asset, and data centres hosting critical cloud computing (including core network points of presence) should be declared national critical information infrastructure.

The importance of data for the digital economy '*data is the new oil'* creates a growing need not only for storing and accessing data, but also for the computing power to process data by using data centres or buying capacity from cloud service providers. Cloud services, through their computing power and frameworks for machine learning, are fundamental for enabling players in the market to exploit the growing potential of 4IR technologies such as Artificial Intelligence (AI), Blockchain and the Internet of Things (IoT).

The increase in demand for storage and processing capacity 'in the cloud' in turn increases the need to establish more data centres to service various industry stakeholders. Data centres are a flexible data storage architecture which delivers an integrated management IT infrastructure, applications and services. In the era of the digital economy, they are an essential resource for economic growth, competitiveness, innovation, job creation, and societal development. To this effect, measures to ensure that South Africa is an attractive host to the data centre industry on the African continent are necessary.

Currently, cloud computing infrastructure (data centre) investment in South Africa is distributed across the country, largely concentrated in big metros located in Gauteng, KwaZulu-Natal and Western Cape, and is mostly foreign-owned. Recognising that data ownership, data sovereignty, and data protection are critical elements for the digital economy, it is important for government to put in place measures to decentralise investments to ensure distribution of opportunities in this area. The small scale of South Africa's current government

data infrastructure is characterised as fragmented and silo-based which implies duplication of effort and a waste of resources.

The supply of energy is central to the establishment and sustainability of cloud computing infrastructure and services. The growth of the technology sector, as well as the adoption of connected devices enabled by IoT, is set to exponentially increase the demand for energy in the next 10 years according to the Presidential Commission on the 4IR. Due to the high-energy consumption and overreliance of the technology sector on energy, many countries have adopted innovative ways of generating and supplying electricity such as the utilisation of green energy in data centres to eliminate reliance on the national grid. The 2018 Norwegian Strategy on data centres, for example, makes provision for generation and distribution of electricity by data centre operators/players.

Digital technologies such as AI, Blockchain and IoT, coupled with big data and data analytics, have the potential to create an exponential impact on developing economies both which is both positive and negative. According to National Treasury, sectors such as manufacturing and services contribute a significant portion to GDP. However, they are at risk of falling behind while the agriculture, tourism and ICT sectors, with a strong potential for employment, only contribute a slightly smaller percentage to the GDP.

To leverage the full potential of the South African economy through digital technologies, government has proposed the establishment and operationalisation of a Digital Transformation Centre (DTC). The DTC will act as a catalyst to lead Digital South Africa. The primary objective of this initiative is to ensure coordination and the prevalence of an integrated innovation and start-up ecosystem that empowers its members and stakeholders. The ultimate intention is to unleash ubiquitous digital transformation in all sectors of the economy, thereby ensuring global competitiveness, and social and economic inclusion. Through this initiative, core engines of growth will converge to enable the digital transformation of the South African economy through the innovation system, the entrepreneurial ecosystem, and the technology ecosystem.

The digital era has brought about a fundamental shift in the global economy, pushing the parameters of innovation and redefining the boundaries of global trade. Moreover, innovations have never been faster paced, more prevalent, or scaled up more quickly than they are now. In order to accelerate the development of local innovations by local technology

SMMEs, government has prioritised the roll-out of digital hubs in most of the under-served rural provinces. A digital hub is defined as a cluster of technology, digital media and internet companies. These hubs will be established as the critical infrastructure required to foster an atmosphere of innovation and creativity and to support digital entrepreneurs through the ecosystem. In the main, hubs focus on rendering support services to early-stage and established businesses, thus enabling them to thrive in a nurturing community, where synergies are created around every corner. They usually consist of specialised zones with specific functions and other basic amenities including, amongst others, applications laboratories and testing stations, market spaces, innovation rooms, and workstations.

Most economically successful countries across the globe have used industrialisation as the preferred route towards sustainable economic and social development. For the country to reap the benefits associated with the digital economy, flexible, effective and efficient tools, that are responsive to the strategic needs of the business sector, investors and other strategic stakeholders, are required. The Special Economic Zone (SEZ) Policy and Legislation (Special Economic Zone Act, Act No. 16 of 2014) was developed for this purpose, as one of the key instruments to accelerate the country's industrialisation agenda. The programme has been designed, amongst others, to attract foreign and domestic direct investment; expand the manufacturing sector (both the primary and secondary economic activities); create sustainable and decent jobs; attract, develop, and retain talent and knowledge; as well as enhance innovation.

In line with the country's Re-Imagined Industrial Strategy, government will need to accelerate the development and operationalisation of distributed ICT SEZs. The objective is to accelerate local technology innovation as well as manufacturing to enable social and economic development and inclusion. This will ensure that the country leverages opportunities associated with the digital economy.

Policy Interventions

10.1.1	*To support the investment in data and cloud infrastructure and services the implementation of digital infrastructure strategies and policies shall be accelerated by government to ensure connectivity with deployment of access and core network infrastructure (such as submarine cables, 5G, fibre).The aim is to facilitate the requisite capacity to support service delivery (sectors such as public service, transport, health care, education, agriculture, and smart cities) and the digital economy.*
10.1.2	*In support of 10.1.1 a model/strategy to consolidate the existing networks of State-owned Enterprises such as SENTECH and Broadband Infraco, shall be*

	developed to form a State Digital Infrastructure Company (SDIC) to provide network connectivity. The SDIC will have access to the excess capacity of government funded ICT infrastructure of Eskom 's telecommunications, SANRAL, Transnet, PRASA and SANREN. The model/strategy shall also take into consideration the implementation of peering for all SITA networks to allow for interfacing with other relevant network services.
10.1.3	*A High-Performance Computing and Data Processing Centre (HPCDPC) shall be established, which will include processing and data facilities and cloud computing capacity and will consolidate existing public funded data centres. The HPCDPC will leverage the existing computing capacity and technical capabilities of the Council for Scientific and Industrial Research (CSIR) and SITA and will operate in conformance with international best practice. The HPCDPC shall have access to the excess capacity of public funded data centres of entities such as Sentech and Broadband Infraco, Eskom and Transnet.*
10.1.4	*The HPCDPC shall provide use-on-demand cloud services for State entities, national departments, provinces, municipalities, metros, SOEs, universities, research centres, civil society organisations, and businesses (South African registered). The connectivity and interconnection of the HPCDPC to all other public datacentres (physical and/or cloud based) will be provided by the SDIC.*
10.1.5	*The HPCDPC shall be replicated with two similar centres to ensure the availability of backup and business continuity in instances where the maincentre comes under cyberattack.*
10.1.6.	*SITA, in line with the e-strategy, shall drive the adoption of digital government services, applications and solutions, with the respective departments, provinces, municipalities, metros, SOEs, and government agencies running and managing their own applications.*
10.1.7.	*A Digital/ICT Special Economic Zones (SEZs) shall be established to support local and foreign investment in data and cloud infrastructure and services. Multinational firms investing in data centres shall be required to make provision for skills and digital technology transfer to ensure benefits and gains from Foreign Direct Investment (FDI).*
10.1.8.	*Data centres may make provision for self-generation energy capabilities to ensure uninterrupted and sustainable operations while reducing total dependence on the strained national electricity grid.*
10.1.9.	*To support SMMEs in the digital economy, strategies and interventions(such as digital hubs and digital transformation centres, supported by open compute and open software) shall be adopted by SITA to enable locally developed applications through collaboration between relevant government departments, agencies, academia and SMMEs.*
10.1.10.	*Investment in data centres and cloud services shall comply with the provisions of broad-based black economic empowerment.*

10.2 Policy issues on Access to Data and Cloud Services

Data has several important features that afford opportunities for socio-economic development and inclusion. In addition, data is essential for descriptive and diagnostic purposes, which are both critical to government for developing future predictions and prescriptions when planning. However, data tends to be held and owned by the main actors who own the service or product offered to the customer or citizens. Various intermediaries also hold significant customer and

citizen data. Simultaneously, the sharing and flow of data within government is limited and restricted, thus depriving government of access to critical insights for economic planning, disease management and crime prevention. Similarly, there is critical data that is held by the private sector which, if shared with government, could enhance government's planning and service delivery capability, without infringing on the rights of citizens.

A large quantum of data is generated by government and its institutions using public funds. However, a significant portion of this data remains inaccessible to many citizens, although such data may be non-sensitive in nature and could easily be used by citizens for scientific, economic and developmental purposes.

Similarly, digital data collected largely remains exclusive to the haves, and thus excludes the have-nots in the periphery of modern economic and social activities. Simply providing internet access is not sufficient. South Africans must have access to quality internet where they are not only consumers but can be inventors and innovators in the digital platforms and ecosystem, and further enable the export of new products and services. Efforts to reduce data cost, and widen quality internet access, must be intensified.

The benefits of data are realised when data is available and accessible to all in an equal and equitable manner. Access to data by all will create new industries and digitally transform traditional industries to be part of the digital revolution.

There is a need for South Africa to develop an open data strategy/framework for the sharing of data, informed by 'Data for Good' principles, to enable access to relevant data for all South Africans including NGOs, and enterprises large and small. The terms and conditions of such access to data will be defined in the open data strategy. The 'Data for Good' principle for NGOs accessing relevant data without paying for access should be considered.

Globally, data that is open is recognised as a critical component of the data revolution for three main reasons. First, the opening of data paves the way for societal benefits. Second, open data has the potential to contribute to social and economic growth whilst ensuring inclusion. Finally, data that is open fosters transparency and accountability between citizens and their governments.

According to the World Bank, many governments have adopted 'Open Data' programmes with the aim of making their digital, machine-readable data available for business and citizens to use and re-use for any lawful purpose. For example, in Europe, the European Union Re-use of Public Sector Information Directive has made it easy to access data. The European Commission published the European Strategy for Data, 2020 in the form of a White Paper, which declares data as a public commodity. The strategy provides that citizens should be empowered to make better decisions based on insights gleaned from non-personal data. It further provides that data should be available to all, whether public or private, big or small, start-up or giant. The intention of the White Paper is to create a single, openly accessible data market that individuals and corporations can all tap into for their own use.

In 2013 the UK Government published its Open Data Program with the objectives informed by the following elements: (i) social and economic growth, (ii) business innovation and the creation of jobs; (iii) inclusive citizen engagement in improving public services, (iv) increased transparency and accountability; and (v) the efficiency and operations of public services.

On the African continent Rwanda has made strides in leading the continent's digital revolution. In 2013 it published the Access to Information (ATI) Law to enable the public and journalists to access information/data possessed by public organs and some private bodies. In 2017, Rwanda published a National Data Revolution Policy which amongst others provides that open data should be published by both public and private actors. The policy further provides for a centralised data portal supported by adoption capacity building programmes in data management, and further provides for elimination of the silo-based approach to the handling of data by government and its entities.

South Africa's National Integrated ICT White Paper provides for the development of a clear Open Government Data Action Plan and Manual through consultation with all relevant stakeholders and will include: (i) information on the types of public information that should be available for everyone to access, re-use and redistribute. It will also clarify the types of information to be made available, such as personal and classified information and data, (ii) a standardised public licence setting out the terms and conditions for using and re-using public data and information, (iii) clarity on the tools and systems to be put in place to ensure that open public data and information is discoverable and searchable, (iv) an implementation plan to establish a single, easy to use, open data government access point, (v) detailed information on how government entities should implement open data policies, the standards required,

and security measures to be put in place to protect data and metadata from interference by unauthorised users, (vi) how government will facilitate innovation and involve citizens in developing software, and (vii) applications to utilise public data.

Recognising the importance of socio-economic development, it is important to give effect to the policy pronouncement made in the National Integrated ICT White Paper that non-sensitive government data should be made available to all citizens to enable innovation and the development of digital solutions that can solve societal problems. These solutions and innovations could also help government to accelerate service delivery to all citizens.

The Presidential Commission on 4IR recommends that government create an integrated data platform with some subset of this being an open big data platform that will make it possible to access digital data housed within a future hyper-scale cloud, with open application programming interfaces (APIs) for those using the data to create products and solutions.

Policy Interventions

10.2.1	*All public data must be captured by default in a digital format.*
10.2.2	*A National Open Data Strategy, anchored on 'Data for Good' principles, shall be developed to:* • *Stimulate digital economic development, innovation, and enablement of SMME development;* • *Address data sharing and interoperability, ownership, data sovereignty, economic rights, integrity and quality;* • *Make provision for the establishment of an open data platform that will give access to all the digital data housed within the HPCDPC, with open APIs for those using the data to create products and solutions for social and economic development;* • *Make provision for the new speciality of open big data brokers to take public data from multiple government sources, and to analyse and exploit these data pools to create products and solutions for social and economic development;* • *Make provision for the sharing of data across all government levels and businesses for the purposes of service delivery and informed policy making;* • *Make provision for a digital trust framework;* • *Give effect to the Open Government Data Action Plan and Manual; and* • *Incorporate principles that data should be open by default; timely and comprehensive; accessible, usable and reusable; comparable and interoperable; and trusted and authoritative.*
10.2.3	*Non-sensitive government data shall be stored in the public cloud of the HPCDP, in line with the existing government data protection and access framework and legislation, to enable universal access.*
10.2.4	*Government shall establish frameworks such as Data Trust to enable sharing of data generated by public and private sectors in a fair, equitable and transparent manner.*

10.2.5	*A model for localised data banks in the HPCDPC shall be developed to enable big data analytics for the development of South African and Afrocentric solutions and innovations.*
10.2.6	*Classification of information, as contained in the Minimum Information Security Standards, shall be reviewed to enable easy access to data for citizens to drive digital economic participation.*
10.2.7	*Government departments and State agencies shall develop their own sector specific data classification guidelines informed by the classification framework of the State Security Agency. In addition, government departments and State agencies shall develop governance frameworks clearly indicating delegation of authority for access to data, the purpose for which the data is required and responsibility for a record of the flow of data in and out of the organisation.*

10.3 Policy Issues on Data Protection

Data is considered a primary asset, and as such must be protected in a manner commensurate with its value. Data security is necessary due to its infrastructure value for the digital economy. More reliance on web-based and digital technologies creates more vulnerability for South Africa and its citizen. Data security is critical in ensuring that data is kept safe from unauthorised access, alteration and distribution.

To date South Africa has adopted a Policy and Legislation Framework on Data Protection and Privacy. The development of this policy and legislation did not take into consideration the context of the digital economy where data is the key driver of societal and economic development.

In accordance with universal personal data protection principles, as provided for in the POPIA and the European GDPR among others, personal data shall be guided by the following principles:

- Lawfulness, fairness and transparency to ensure that the collection of data happens within the prescripts of the law and in a transparent manner;
- Purpose limitation, to ensure that the purpose for which data is collected is clearly articulated and is only collected as long as necessary to complete such a purpose;
- Data minimisation, to ensure that data is processed only for the need to achieve its processing purposes;
- Accuracy and completeness, ensuring that data subjects are enabled to rectify and where necessary erase data to ensure its accuracy and completeness;
- Storage limitation, ensuring that data is not stored longer than necessary; and
- Integrity and confidentiality, to prevent unauthorised alteration and access.

Policy Interventions

10.3.1	*Processing of metadata on personal information shall comply with privacy provisions as contained in the POPIA and other data protection legislation.*
10.3.2	*Data protection measures in South Africa shall comply with POPIA, PAIA, ECTA, and other data protection policies and legislation, as well as international best practice.*
10.3.3	*The ECTA shall be reviewed where necessary to align it with cyber security policy and legislation.*
10.3.4	*Data generated by government and State entities shall be stored in the HPCDPC in conformance with security measures as defined by the Minister of State Security to safeguard integrity and security, and ensure collective rights over collective data.*
10.3.5	*The Minimum Information Security Standards and Protection of State Information Legislation shall be reviewed, where necessary, to enable protection of sensitive data in the digital economy.*
10.3.6	*For the purpose of protection of sensitive data, government shall use private cloud for sensitive data in line with the existing government data protection framework including PAIA.*
10.3.7	*Relevant regulatory institutions shall develop regulatory and monitoring frameworks to give effect to data residency.*

10.4 Policy Issues on Localisation and Cross Border Data Transfers

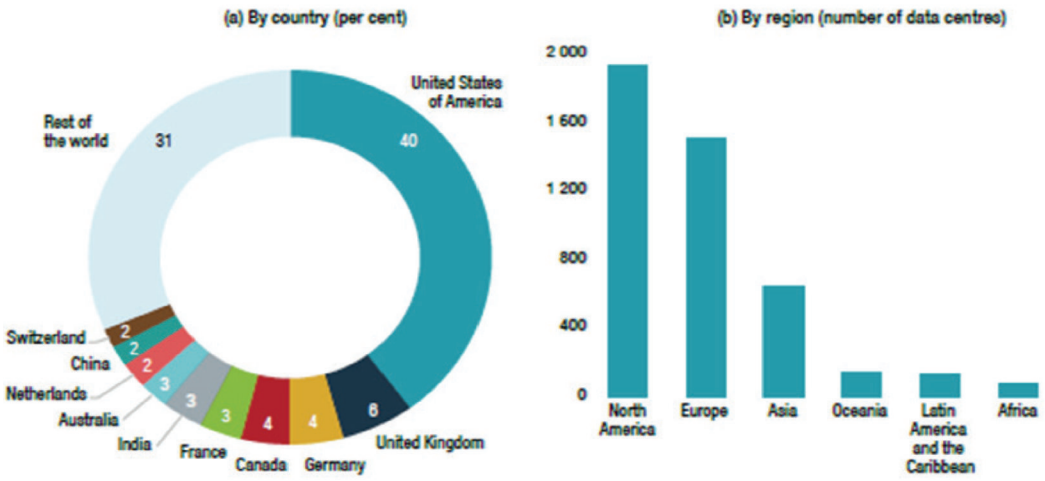
Localisation generally refers to requirements for the physical storage of data within a country's national boundaries, although it is sometimes used more broadly to mean any restrictions on cross border data flows.

To ensure South Africans derive socio-economic value from data, it is prudent to address key policy issues such disclosure of ownership arrangements, location factors, and transfer and data preservation.

According to UNCTAD, 2019, the dominance of North American, European, and Asian technology giant companies is shown by the concentration of data centres. Data centres house the data value chain and monetisation. Figure 2 shows South Africa and Africa as unequal participants in data centres.

26

Figure 2: Geographical distribution of colocation data centres, February 2019



Source: UNCTAD (2019, p. 12)

The possible implication of the above is that data generated in Africa and South Africa is mostly stored in foreign lands and, where stored locally, is owned by international technology giant companies.

It is essential to recognise that data is a tradable commodity which is a central productive force for the development of the digital economy. Technology companies primarily make use of 'freemium' business models, where customers access services free of charge in exchange for their data being collected. This data is then sold globally for advertising purposes. In this regard, countries have developed policies and legislation that limit the unrestricted flow of data outside of their borders.

In digitised, data-driven economies, companies and individuals have found innovative ways to conduct data-related business transactions in countries where they do not have offices or a physical presence. This creates a challenge in determining where digital businesses derive revenue and pay taxes and makes it easy for a country to be deprived of its due tax revenues. South Africa is facing this same challenge.

Adam Smith, an economist, said that taxes should be efficient, certain, convenient and fair. To determine the appropriate tax to be paid, however, there is a need for adequate information about each company, its business activities and the revenues accruing therefrom. This needs to be managed in a manner that cannot be seen to be discouraging to investment because multinational companies tend to seek countries that have favourable tax policies.

For South Africa to derive tax revenue from digital activities, appropriate frameworks and policies need to be in place, informed by best international practices, while also taking into account the need to grow the data-driven economy by combining foreign investment and localised initiatives. Notably, the South African Receiver of Revenue has indicated that work is already under way in this area.

South Africa supports the free flow of information and data as articulated in the POPIA. However, the development and growth of the digital economy makes it necessary for South Africa to restrict and protect some of its citizen's data to effectively participate in the global digital economy. This challenge, with data being the central productive force in the digital economy, compels the South African Government to play a more central role in the collection, dissemination, and analysis of data, understanding that key economic advantages are contained within it.

South Africa must also derive socio-economic benefits from its data. Essentially, the data must be of a common good for all residing in South Africa. However, it remains unclear how data generated through intellectual activities of varying degrees and types would be correctly categorised in terms of Intellectual Property Rights (IPR).

Recognising that data storage is not limited to geographical location, consideration should be given to measures that ensure that cross-border data transfers do not transgress the national security and privacy protection laws and other related policies and legislation of South Africa.

Policy Interventions

10.4.1	*All data classified/identified as critical Information Infrastructure shall be processed and stored within the borders of South Africa.*
10.4.2	*Cross-border transfer of citizen data shall only be carried out in adherence with South African privacy protection policies and legislation (POPIA), the provisions of the Constitution, and in compliance with international best practise.*
10.4.3	*Notwithstanding the policy intervention above, a copy of such data must be stored in South Africa for the purposes of law enforcement.*
10.4.4	*To ensure ownership and control:* • *Data generated in South Africa shall be the property of South Africa, regardless of where the technology company is domiciled.* • *Government shall act as a trustee for all government data generated within the borders of South Africa.* • *All research data shall be governed by the Research Big Data Strategy of the Department of Science and Innovation (DSI).*

- *All data generated from South African natural resources shall be co-owned by government and the private sector participant/s whose private funds were used to generate such, and a copy of such data shall be stored in the HPCDPC.*
- *Ownership and control of personal information and data shall be in line with the POPIA.*
- *The Department of Trade, Industry and Competition through the Companies and Intellectual Property Commission (CIPC) and the National Intellectual Property Management Office (NIPMO) shall develop a policy framework on data generated from intellectual activities including sharing and use of such data.*

10.5 Policy Issues on Cybersecurity Measures

South Africa's economy is digitising at a significantly fast pace. This is likely to increase the threat of cybercrimes and has the potential to exponentially impact negatively on the economy. The digital economy is about sharing and using common infrastructure and digital platforms. The internet, over which the data is transmitted between digital ecosystem actors, thrives on interconnectedness and extensive networking. This brings greater vulnerability to the whole ecosystem, be it from indigenous or exogenous attacks. The tightening of information and cyber security systems in both public and private domains must be a top priority.

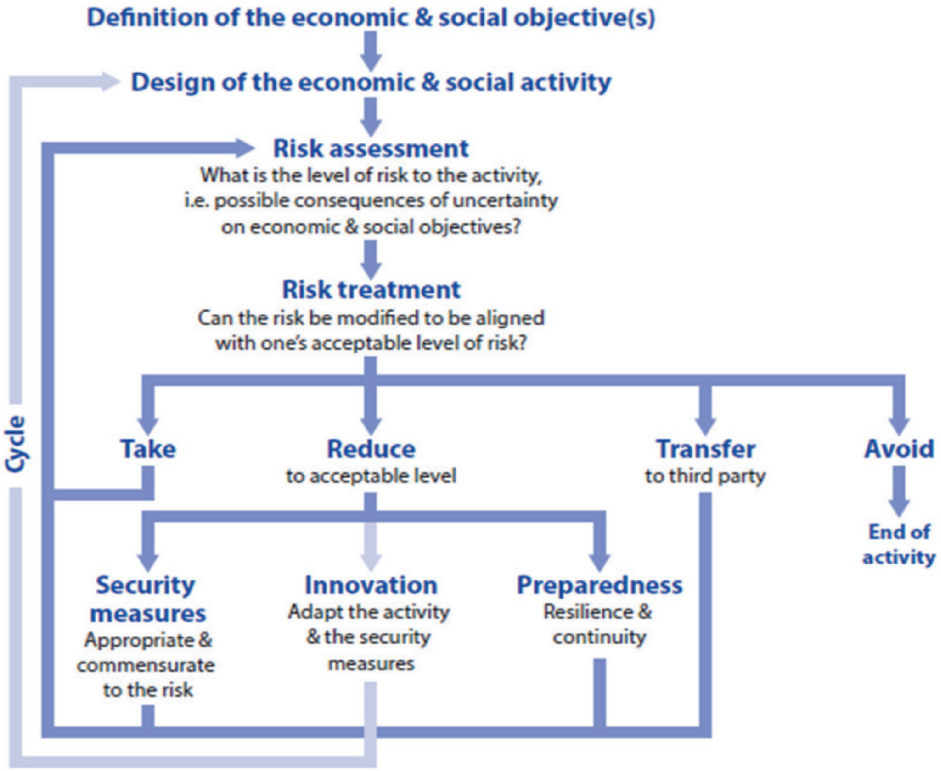
Considering the increasing importance of cloud computing services as well the role they play in the digital economy, a framework to manage the risks related to the provision of such services becomes as important as the need to promote the rapid deployment and adoption of such services.

South Africa has been ranked third in the world for online crime. According to the South African Banking Risk Information Centre (SABRIC), South Africa's annual loss is estimated at R2,2 billion ($156 million), which adds insult to an already economically injured economy.

As digital citizens are more and more empowered with data about their location and activities, issues of privacy become necessary. Consideration needs to be given to privacy and protection from systems that gather data, which pose a continuous security challenge.

The new reality, where there is wide deployment of digital technologies in all sectors of the economy and society, compels countries to develop digital risk management frameworks. The OECD's Digital Security Risk Management for Economic and Social Prosperity proposes a digital security risk management cycle which is reflected in Figure 3.

Figure 3: Digital security risk management cycle



Source: OECD (2015, p. 36).

For South Africa to fully leverage the opportunities presented by 4IR technologies such as data and cloud computing, a fully integrated strategic approach to digital risk management is fundamental, and must be an integral part of national security, planning and response. This can be complemented by a social compact based on public-private partnerships (such as legislators, regulators, service providers and communities) for effective policy implementation and ensuring public trust.

Policy interventions

10.5.1	*To ensure confidentiality, integrity and availability, the National Cybersecurity Policy Framework (NCPF) and other related policies, legislation and international best practice shall guide the implementation of initiatives and measures (national firewall deployed, distributed access platforms such as Science DMZ and fit for purpose cyber-security measures aimed at preventing cybersecurity risks and threats).*
10.5.2	*The NCPF shall be reviewed where necessary to ensure it is responsive to the threats and risks associated with digitisation.*
10.5.3	*The Minister shall, where necessary, take appropriate measures to ensure that the Cybersecurity Hub is capacitated to respond to threats and risks associated with digitisation.*

10.5.4	*Cybercrime legislation shall provide for enforcement and sanctions against cybercrimes.*
10.5.5	*Cybersecurity awareness initiatives shall be developed and implemented for the public so that South African citizens are aware of cyber risks and are educated on safety measures in the cyber space.*

10.6 Policy Issues on Governance and Institutional Mechanisms

Data governance is referred to as an exercise of authority, control, and shared decision making which includes planning, monitoring and enforcement over the management of data assets either within one organisation or across different organisations that share an interest in common data assets (OECD, 2019).

A data governance model must support existing and new processes to ensure proper management, protection, production and usage of data through its life cycle in a collaborative and united approach to managing valuable data assets. In this regard consideration should be given to the development of a framework on ethical guidelines to ensure elimination of the bias associated with digital technologies.

Harmonisation of technical standards across the data value chain is critical in order to optimise the benefits of data. To date, government has developed an interoperability framework through its e-Strategy of 2017. What is currently lacking is the interoperability framework which will enable sharing of data between government and the private sector.

The current data governance ecosystem is highly fragmented and has a silo-based approach, making data unmanageable and difficult for users to control. South Africa has a broad landscape of regulations and regulating bodies. Multiple government actors collect data across the country. This data is stored in separate platforms, largely as refined and production data. The lack of interoperability limits South Africa's participation in the digital economy. Looking at the current and future needs of the country, there is a need to consider, among others, amendments to the Statistic Act, Act No. 6 of 1999, which established Statistics South Africa (Stats SA). The amendments would broaden the scope of Stats SA to oversee the central collection, storage, digitisation, and analytics of all government data in South Africa.

There is at times a duplication and overlap in the mandates of several of the country's current regulatory bodies. The quest to derive socio-economic value out of data presents South Africa with an opportunity to establish one regulator from a number of regulatory institutions regulating information/data as well to review the mandates of the institutions responsible for

data collection and governance. The rapid trend of converging technologies makes a strong case for reviewing the country's current regulatory bodies and considering a case for merging and consolidation.

To ensure the sustainable growth and development of the digital economy and its success there is a need to ensure that the various regulatory institutions' mandates are enhanced and aligned. This would cover the restructuring of current institutional capacity and the building of new capacity, as well as establishing or promoting physical systems which will play a key role in the 4IR.

Policy Interventions

10.6.1	*The Minister shall establish an Advisory Council consisting of private and public representatives and academia, to advise amongst others on:* • *Data management standards, guidelines, best practices and the use of data for innovation and economic activities;* • *Development of a regulatory framework for the management of data and cloud services;* • *Strategic data sets that can stimulate innovation and the economy, and support service delivery;* • *An interoperability framework between government and business; and* • *Policy considerations on an AI code of ethics.*
10.6.2	*A review shall be undertaken of the existing regulatory authorities mandates with a view to establishing a single data regulator, reporting to the Minister of Communications and Digital Technologies.*
10.6.3	*An institutional framework shall be established to manage the government's High Performance Data Centre which will include a review of the mandates of existing government agencies and government departments to enable:* • *Interoperability;* • *Integration; and* • *Harmonisation of data standards.*
10.6.4	*The Department of Public Service and Administration shall develop norms and standards on data for the public service and administration that will, amongst others, address metadata management, data quality management, data classification and data security including information management and information technology in the public service, taking into consideration State security provisions.*

10.7 Policy Issues on Competition

The digital economy requires a competition policy that will level the playing field, enabling the creation of, access to and capturing of value from data and cloud services. The European Union is proposing a Digital Services Act (DSA), which introduces a new ex ante regulatory regime (a regime based on forecasts rather than actual results) for digital platforms. The main goal is to create balance between competition, innovation and protection.

For South Africa, existing legislative frameworks would need to be adapted to provide for competitive and contestable markets. This is necessary because current polices and legislation were not designed to regulate competition in the digital economy. The existing polices and legislation should be broadened to consider, for example, consumer choice, market structure, switching costs and lock-in effects.

On 07 September 2020, the Competition Commission published a paper titled Competition in the Digital Economy for public comment. *The paper argues that, 'the arrival and rapid rise of the digital economy presents the country with an opportunity to reverse the pervasive, triple scourge of unemployment, inequality and poverty. But in order to harness the promised benefits of digitalisation, there is a need to create a commercial and regulatory environment designed to extract those benefits and distribute them in a way that ensures inclusive economic growth, that is (i) increased and meaningful employment; (ii) equality; and (iii) shared prosperity'.*

The paper further warns against the risk of global concentration which is characterised by further marginalisation of vulnerable countries and businesses. '*Therefore, intentional regulation is required to avoid outcomes that could harm the development of small businesses, consumers and ultimately the economic growth so needed in South Africa's developing economy'.*

Data Concentrations

The data and cloud computing market structure is dominated by a handful of large multinational companies. The concentration of data within this limited number of corporations poses a risk as it limits possibilities for the extraction of public value from data. Furthermore, this lack of market competition has given consumers few alternative choices for the protection of privacy, and none are likely to appear.

Interoperability has the potential to be used not only for data cooperation, but also as a competitive lever to counteract data concentrations and allow new data market entrants to arrogate network effects. Many cloud providers do not consider open source standards, which are mainly used by the public cloud providers, but instead opt for proprietary standards, which make it difficult for smaller organisations and companies to move applications and workloads back and forth between private and public clouds. Limited migration between clouds is

preventing organisations and companies from selecting the best cloud services and avoiding vendor lock-in.

The playing field is therefore not level and does not allow for equal opportunity of participation between new entrants, including SMMEs, and big companies in South Africa. As argued by the Competition Commission's paper on Competition in the Digital Economy, '*the accumulation of big data – which has become a most valuable asset in the digital economy – coupled with network effects, can confer market power and a durable competitive advantage*'.

New entrants, including SMMEs, do not have the financial capacity to own and operate the sophisticated information technology systems found in large organisations. This limits their ability to offer their local knowledge and specialised talents to customers, big or small. They are also not adequately resourced to establish infrastructure for the storage, management and processing of data or to develop economies of scale that would help them to be competitive. New entrants, including local SMMEs, do not have access to data storage facilities such as cloud or other data centres, thus rendering them unable to collaborate with partners elsewhere in the world to share ideas, expand their horizons, and dramatically improve their job creation abilities.

Market Power

The Competition Commission paper further argues that '*market power has become the source of several concerns raised in the digital economy,'* and highlights the following issues:

(i) Vertically integrated digital firms can benefit from owning a platform and, at the same time, competing with sellers on that platform. This enables the platform owner to use the information it collects from the seller to its advantage and the disadvantage of the seller;

(ii) Vertical integration also incentivises self-referencing: an act by which digital platforms will give preferential treatment to their own services over the services of other companies and as such maintain their positions of dominance;

(iii) Conglomeration has the potential to negatively impact inclusive growth, even where several big players are competing. This is particularly concerning in the South African context where market concentration levels are already high, and the likely impact of increased conglomeration raises barriers to entry for potential entrants;

(iv) Online resale price maintenance has also been investigated in European cases resulting in decisions against manufacturers of consumer electronics.'

First Mover Advantage

Industries, including mobile operators in South Africa are providing Internet of Things (IoT) gadgets for consumers by tapping into data that they have generated through the provision of telecommunications services over time. This data, when aggregated and analysed, can provide valuable insights across a wide range of use cases. Through the provision of these IoT services, mobile operators and the industry amass more data which has the potential to give them significant dominance in the data market. Data and cloud computing have the potential to create vertically integrated entities, which can potentially limit entry into markets by new players, including SMMEs.

Policy Interventions

10.7.1	*Competition law shall be reviewed to address specific challenges relating to dominance by a few established players, and anti-competitive behaviour which might arise within the data and cloud environment, taking into consideration the FAIR (Free, Accessible, Interoperable, Reusable) principles of data.*
10.7.2	*Legislation shall also be reviewed to ensure that local companies have a fair and equitable chance of competing with their global counterparts.*
10.7.3	*To support competition, the Open Data Strategy shall enable the development of a regulatory framework for exportability, interoperability, data portability, and data trading and sharing. The strategy shall also inform the development of sector-specific regulations.*
10.7.4	*Sector-specific regulators, supported by policy from relevant departments, shall develop regulatory frameworks to facilitate disruption for the purposes of fostering inclusion and reducing market concentration.*

10.8 Policy Issues on Skills and Capacity Development

The challenge for South Africa is to ensure that all its citizens are able to take advantage of the ever-expanding number of opportunities presented by 4IR technologies, such as data and cloud computing. Innovative capacity building initiatives and the strengthening of digital skills will play a pivotal role in meeting this challenge.

Recognising that South Africa has a young population and a high unemployment rate, any policy that supports the adoption of digital technologies to enable social and economic development must look at the development of people and skills. Such policies necessitate a skilled, capable and technologically advanced workforce which is continuously learning and keeping pace with the rate of development and the change these technologies bring about. Smart and connected societies are fast becoming the norm, and South Africa has critical issues to solve in attaining this goal.

For South Africa to fully realise the benefits of a digital economy, it should adopt an integrated skills development plan and programme, designed to ensure the building of competencies that will enable the majority of South Africans to understand the fundamentals of data and cloud computing, and how to access these to exploit economic opportunities.

Data analytics generates new insights, creating new knowledge and paving the way for automated decision making. Various technologies are used to generate data analytics. Amongst other competencies, South Africa needs to develop competencies in the technologies and techniques that enable analytics. This is essential on two fronts: the first front being to help eliminate the bias inherent in the technology, which could be harmful to members of South African society; and the second front being to position South Africa as a developer of some of the digital technologies and thus enhance its participation as an equal participant in the digital economy.

Policy Interventions

10.8.1	*The Minister, in consultation with other relevant ministers, shall develop capacity building programmes and initiatives on big data and cloud computing in line with the National Digital and Future Skills Strategy, focusing on:* • *Basic (for individual users);* • *Intermediate (for corporate users);* • *Advanced level (for developers of applications and services); and* • *Government (for public service and government agencies).*
10.8.2	*Government shall partner with the private sector and training institutions to provide digital skills for citizens, including SMMEs.*
10.8.3	*Government shall partner with various international organisations with relevant skills, utilising the bilateral and multi-lateral agreements that South Africa is party to.*

10.9 Policy issues on Research, Innovation and Related Human Capital Development

The digital economy, as characterised by the application of 4IR and data technologies, is evolving at a pace that has the potential to leave South Africa behind by several years if not given an urgent and appropriate response. Any country's response to current and future technological development can only be guided by the extent of its research and development capacity.

One of the country's technological development plans is the establishment of the AI Institute, as recommended by the Presidential Commission on 4IR. This will be the facility for training, research and development. The AI Institute will advance the use of AI in tackling challenges that South Africa faces. Data is central to the application of AI and is the key asset. The use of AI requires that data must comply with the FAIR principles: be findable, accessible, interoperable and re-usable (Wilkinson et al., 2016). The Data and Cloud Policy will empower the AI Strategy which will be pursued in the AI Institute.

The 2019 White Paper on Science, Technology and Innovation provides for a focus on using Science, Technology and Innovation (STI) to accelerate inclusive economic growth, make the economy more competitive and improve people's daily lives. It aims to help South Africa benefit from global developments such as rapid technological advancement and geopolitical and demographic shifts, as well as respond to the threats associated with some of these global trends.

The establishment of dedicated research and development capacity is critical for the development of human capital to derive value from data and cloud computing, and to establish world standards and reliable cyber-infrastructure. In addition, research and development capacity is important to ensure investment in current and future data initiatives to support the digital economy.

Policy Interventions

10.9.1	*The Department of Science, Innovation and Higher Education, in collaboration with the Department of Communications and Digital Technologies, shall be responsible for the R&D on big data and cloud computing, in line with the business model for data and cloud research as articulated in the White Paper on Science, Technology and Innovation.*
10.9.2	*The Department of Communications and Digital Technologies shall establish an institutional mechanism to enable South Africa to participate in the recent emergence of institutions studying the impact of 4IR technologies such as the AI Institute.*

11. Review of the Policy

This Policy shall be reviewed, as and when necessary, to enhance South Africa's digital economic development, and to ensure compliance with new domestic laws, where applicable, as well as international standards and norms.

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