Submission Cloud Infrastructure Service Provider Africa Working Group of the
Digital Council Africa
on the
Draft National Policy on Data and Cloud

The Director-General
Department of Communications and Digital Technologies
iParioli Office Park
1166 Park Street,
Hatfield, Pretoria
0001

Attention: Ms C Lesufi
Director, Telecommunications Policy

By email: DataCloudpolicy@dtps.gov.za

1 June 2021

Dear Ms Lesufi

WRITTEN SUBMISSION – PROPOSED NATIONAL DATA AND CLOUD POLICY

1. The Digital Council Africa (**DCA**), through its Cloud Infrastructure Service Providers Africa (**CISPA**) Working Group, hereby submits written comment on the proposed National Data and Cloud Policy (the **Policy**) published in Government Gazette No. 44389 on 1 April 2021 by the Department of Communications and Digital Technologies.

2. The Council would like to make further representations on the Policy hereby indicates its willingness to participate in any hearings to be held pursuant to this phase of the consultation process.

3. As part of a global alliance and as an independent, not for profit organisation, we believe that we have significant insight into the multiplicity of issues that cuts across our membership as a result of our interface with government, private entities, regulatory bodies, and various industry organisations.

Yours sincerely

Mike Silber
Chair
CISPA Working Group

Avela Gronemeyer
Deputy Chair
CISPA Working Group

SUBMISSION

Cloud Infrastructure Service Providers Africa Working Group

of the

DIGITAL COUNCIL AFRICA

on the

DRAFT NATIONAL POLICY ON DATA AND CLOUD

Submission Cloud Infrastructure Service Provider Africa Working Group of the
Digital Council Africa
on the
Draft National Policy on Data and Cloud

INTRODUCTION

1 The **Digital Council Africa** (**DCA**) is an industry association with a strong focus on digital infrastructure. It endeavours to support public and private stakeholders with issues such as policy and regulation, best practice, and minimum standards through a collaborative effort. Member engagement is encouraged through participation in events and working groups. We offer members an opportunity to network and collaborate and discuss best practice frameworks that is in the best interest of all, solving complex issues through dialogue and policy adoption. Furthermore, we encourage dialogue between government and private sector from a platform that is independent and product agnostic.

2 Finally, we have a clear mission is to see broad-based investment in digital skills by all stakeholders, thereby enhancing the lives of all people living on the continent of Africa to enable them to participate in the digital economy.

3 The DCA convened various entities active in the Cloud Infrastructure industry, who have formed the Cloud Infrastructure Service Providers Africa (**CISPA**) Working Group under the auspices of the DCA.

4 The DCA and the CISPA Working Group thank the Depart of Communications and Digital Technologies for the opportunity to engage on the proposed National Data and Cloud Policy (the **Draft Policy**) published in Government Gazette No. 44389 on 1 April 2021.

5 The digital transformation of our society and the increased creation of and reliance on data, much of which is stored and processed using cloud infrastructure has resulted in a need to formulate policy to address these issues at a national level. The DCA is particularly encouraged that these important issues are receiving the attention they require. This Draft Policy seeks to enable South Africans to realise the socio-economic value of data through the alignment of existing policies, legislation, and regulations. The Draft Policy further seeks to put in place a conducive and enabling environment for the data ecosystem to thrive.

6 Our submission will follow the format set out in the Draft Policy.

Submission Cloud Infrastructure Service Provider Africa Working Group of the
Digital Council Africa
on the
Draft National Policy on Data and Cloud

POLICY ISSUES ON DIGITAL INFRASTRUCTURE (CHAPTER 10.1)

7 Overarching Comments

7.1 The Working Group has taken note of the objectives of the Draft Policy in respect of digital infrastructure and welcomes the attention given to digital infrastructure. At the same time, the Draft Policy makes certain statements that do not appear to be based on empirical data and the Working Group is concerned that there is a data deficit underlining certain of the statements as well as key proposed policy interventions.

7.2 The Draft Policy further conflates private and public infrastructure and seeks to treat both in an equivalent manner. Specifically when it comes to the treatment of "digital infrastructure of critical scale", the Working Group is concerned that the notion of "critical scale" is not adequately defined and the proposed intervention of such infrastructure being "declared a national strategic asset" is lacking in detail as to how such a declaration will be affected, particularly in the light of the existing provisions of the Critical Infrastructure Protection Act, 2019. The proposal in the Draft Policy does not follow the processes outlined in the Act, which has yet to come into effect.

7.3 The Draft Policy goes on to suggest that the concentration of cloud computing infrastructure in metro areas is a negative circumstance. This, however, ignores the key drivers for the location of cloud infrastructure: availability of power, demand from markets, access to critical skills and proximity to customers. Critical infrastructure must be accessible to support staff (both customer and provider) within a matter of minutes and travels delays cannot be accepted.

8 Specific Comments on Proposed Policy Interventions

8.1 The Working Group was generally supportive of the proposed policy intervention 10.1.1, however noted that the Draft Policy did not indicate any of the modalities through which strategies and policies will be accelerated? There are a number of such strategies and policies that are already in place, however progress has been slow and the Draft Policy does not indicate how this will change.

8.2 The Working Group noted the proposed intervention in 10.1.2. The Working Group appreciates government seeking to maximise the return on its existing investments. The Working Group noted that the Department made reference to Telkom infrastructure in its presentation to the Working Group and would appreciate clarification from the Department in this regard.

8.3 The Working Group took note of the proposal in 10.1.3. Subject to the comments below regarding a possible concentration risk and the potential for the reduction in competition, the Working Group is supportive of the state maximising the use of existing assets, procured through revenue derived from taxpayers. However, parts of the Draft Policy seems at odds with this objective of frugality and maximising return and seem to suggest that a new High-Performance Computing and Data Processing Centre (**HPCDPC**) will be constructed and replicated (10.1.5). In addition, the Draft Policy proposes (at 10.1.4) that the tax-payer funded HPCDPC will compete with private sector data centres. This raises serious concerns regarding competition (see our comments in respect of Chapter 10.7 below).

8.4 The Working Group queries the technical rational for replicating the HPCDPC (10.1.5) and suggests that the purported reason for this replication (protection against a cyberattack) does not actually have a solid technical underpinning and will not achieve the desired result.

8.5 The Working Group noted the suggestion regarding the creation of Special Economic Zones and welcomed this suggestion, provided such zones are located in geographies conducive to establishing cloud infrastructure. Seeking to locate these in rural areas is likely to be counter-productive.

8.6 The Working Group noted the recommendation regarding self-generation of power (10.1.8), however noted that this is largely dependant on the wheeling of power through the national and local grids and there have been significant delays in the implementation of wheeling mechanisms, as well regulatory obstacles to self-generation. The Working Group recommended the Department co-ordinate with the Department of Mineral Resources and Energy in this regard.

8.7 The Working Group and its members noted that they already comply with the provisions of applicable broad-based black-economic empowerment policy and law.

POLICY ISSUES ON ACCESS TO DATA AND CLOUD SERVICES (CHAPTER 10.2)

9 <u>Overarching Comments</u>

9.1 There are misconceptions in the approach to data ownership set out in the Policy. To be clear, most business-related cloud providers expressly state in their contracts that they do not make ownership claims over the data that they hold in their cloud services. Public sector data can be made open and accessible to citizens and businesses irrespective of the technology which is used to process the data,

as is increasingly occurring in the European Union pursuant to the EU's Open Data Directive. The policy is silent about ownership of data. The reference to the constitution and the other acts such as POPIA means that it subjects itself to these as an enabler. It does mention that government is the custodian (meaning guardian or overseer) of the data that generates in the country. This does not imply that they claim ownership of the data. Government however do own data which they generate in execution their day-to-day operations. This public sector data is what Government will mine in order to improve their decision making regarding the economy and service delivery. The view of Data Ownership in the document needs to consider basic human rights as enshrined in the Bill of Rights and other international standards and treaties that allude to data belonging to citizens.

9.2 One of the typical components of a sound strategy is the recognition of governance in the process of adoption and successful implementation of policies and regulation. A comprehensive approach to all governance aspects, including aspects related to data is important for the adoption of a vibrant digital economy. Appropriate governance of data has significant benefits and, through the right policies and management processes as well as oversight will result in the positive impact the policy sets out to achieve. ISO/IEC 38505-1 provides guidance that may be of assistance for the Policy.

9.3 ISO/IEC 38505-1 sets out principles for governance of data. It further emphasises the need to weigh the risks and opportunities related to data across the lifecycle to extract the appropriate value from data in a fair and principled manner while protecting both the data assets and the interest of relevant stakeholders. It is recommended that this standard should be considered while strengthening the governance components of the strategy.

9.4 One area, for example, that may benefit the Policy is the use of a common data life cycle definition and concept across all the policy areas. ISO/IEC 38505-1 uses a simplified life cycle that includes the elements of collection, use in decision making, sharing, reporting distribution, and disposing. The Policy in its current form only touches on some of the parts of the data lifecycle and sometimes only parts of these elements are described, and it would benefit the policy to have the golden thread from governance through management to implementation referring to a common, consistent approach. ISO/IEC 38505-1 places an emphasis on the constraints on the data life cycle and a particular focus on risk management, a key aspect of many of the more successful policies.

9.5 Similarly, it may be beneficial for DCDT to follow and potentially influence (through engagement with

the South African Bureau of Standards) the development of ISO/IEC WD TS 38505-3 Information technology — Governance of data — Part 3: Guidelines for data classification. This guidance standard is expected to be published this year. It illustrates the considerations for modern data classification approaches and emphasises a risk-based approach to classification, the application across the life cycle of data and the consideration of other facets of data other than the often-used confidentiality, integrity, and availability of data as focus for classification. With zero trust approaches and the diminishing effectiveness and applicability of perimeter defence paradigms when it comes cloud and data, the risk-based approaches are considered good practice.

9.6 Industry understands from the Policy that reviews of the categorisation in the Minimum Information Security Standards and Protection of State Information Legislation will be conducted and hope that the above observations may provide some assistance in such reviews.

POLICY ISSUES ON DATA PROTECTION (CHAPTER 10.3)

10 Overarching Comments

10.1 There are three main stakeholders that are affected when it comes to the privacy and ownership of data as depicted in the diagram below. Their needs, wants and security must be satisfied, and this will require government to put in place the necessary mechanism to ensure that data can be protected and be secured. Government should therefore also consider the Data sovereignty requirements and put further mechanisms in place to ensure that data is stored within the borders of the country and that cross-border data transfer is well controlled.

Security	Privacy, confidentiality and ownership	Competitive edge, growth and survival	Economic progress and well-being of citizens
Needs	Protecting the privacy of individuals	Protecting the intellectual property of businesses	Protecting the data government and the nation
		Control over digital assets	Control over digital assets
Wants	Control over data	Control over data	Control over data
Stakeholders	Individuals	Businesses	Government
Concerns	Worried about the confidentiality of their private lives and the security of their personal data Personal data being collected by business and stored without their consent	The risk of not having control over their intellectual property can be detrimental to business growth and survival	The risk of not having control over the nation's data can be detrimental to economic progress and the well-being of the citizens

10.2 The Draft Policy proposes a mechanism that underpins the existing service delivery capability with a digital mechanism in order to address stakeholder needs in a digital manner and provides a platform that will enhance citizen participation in government service delivery through innovation and other means.

10.3 The citizenry has long been transformed with almost everyone having access to a digital device from where they can access Government Services. When one studies the "data story" explained in the document, it becomes clear that Government is aiming to drive the digitalisation processes through a focus on data, platforms, and cloud.

10.4 **Key Question:** Should this policy be explicit about who owns what data as there is other legislation that clarifies this and if so, what legislation should be amplified.

- 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.

Declare data as a **public commodity**	Make their digital, **machine-readable data available** for business and citizens to use and re-use for any lawful purpose	Create a **single, openly accessible data market** that individuals and corporations can all tap into for their own use.

- South Africa's National Integrated ICT White Paper provides for the development of a **clear Open Government Data Action Plan and Manual**

Information on the types of public information that should be available for everyone to **access, re-use and redistribute**	A **standardised public licence** setting out the terms and conditions for using and re-using public data and information	Clarity on **the tools and systems** to be put in place to ensure that open public data and information is discoverable and searchable
An implementation plan to establish a **single, easy to use, open data government access point**	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	How government **will facilitate innovation** and involve citizens in developing software, and applications to utilise public data

- Presidential Commission on **4IR recommends**

Create an integrated data platform	**Hyper-scale cloud**	**Open APIs**

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

POLICY ISSUES ON LOCALISATION AND CROSS BORDER DATA TRANSFERS (CHAPTER 10.4)

11 Overarching Comments

11.1 The Policy refers to, and appears to be influenced by, a strong data localisation model and seems to follow a "nationalisation of data model."

11.2 Industry agrees that data is a valuable and important resource, and that South African public and private sectors must harness, control, and take advantage of it. However, the approach should consider that applying broad brush localisation and ownership mandates will slow down South Africa's digital transformation and will have a significant negative impact on FDI. Multinational players will be reluctant to invest in a siloed digital economy which does not allow for the free flow of data. Local operators will be confused about how they can use, and exploit data given the broad-brush, prescriptive, and sometimes inconsistent data ownership and classification proposals. Therefore, industry view is that the Draft Policy should also promote what is working well globally and in South Africa. In this context, there is South African examples where there has been a real partnership between the South African Government, technology/cloud providers (e.g., in the Government Cloud) and the indigenous technology community. This approach of partnerships is proving to be successful in driving local digital transformation.

11.3 There is a tension between the application of data localisation mandates, and the important objective set out by the Draft Policy to harness the power of data to effectively participate in the global digital economy and to remove regulatory barriers. Difficulty lies in finding the right balance between unrestricted flow of data and wide-reaching data localisation mandates. Countries internationally address this balance in various ways for different reasons, leading to the development of a number of data localisation 'tectonic plates' across the globe. As drafted, the Draft Policy appears to require the localisation of broad categories of information. Such extensive localisation requirements, while often well-intentioned, can be damaging to the local economy, difficult to implement, and unable to address the primary privacy and security concerns associated with data processing.

11.4 The Draft Policy refers to countries that have "developed policies and legislation that limit unrestricted flow of data outside of their borders", having recognised that "data is a tradable commodity and will be a central productive force for the development of the digital economy." The Draft Policy also states that wide categories of data ("Sensitive Data") must be stored in South Africa, on a private cloud.

11.5 An emphasis on data localisation policies is likely to have detrimental impacts on sectors that are premised on cross border data flows for success (such as the financial services and technology industries). Extensive localisation requirements can negatively impact the functionality of cloud-based services (reducing resiliency and hampering ability to identify security risks across borders).

11.6 As discussed throughout this response, industry considers that the Draft Policy should be aligned with the proposed best practice to identify the risks relevant to a certain set of classified data (rather than category of data) and make decisions on localisation as a result. For example, the particular risk in a set of classified data may relate to confidentiality, extra-jurisdictional access, risk of destruction or non-availability. Then the process of risk mitigation should be undertaken in each case and the risk mitigation plan could, for example, state that data of a certain classification needs to be encrypted with keys held in a secure public key infrastructure with a specified level of crypto security. Such data may need to be available to missions abroad even if there may be a temporary outage of communication and therefore should be stored on a public cloud service in this encrypted for to mitigate the unavailability risk.

12 International Comparisons

The Centre for Internet and Society, India, has studied 18 countries which have begun to implement restrictions on the cross-border flow of data. It recommended that given the complexity of technology, the interconnectedness of global data flows, and the potential economic and political implications of localisation requirements, approaches to data sovereignty and localisation should be nuanced. It also helpfully set out a number of steps which it recommends for India (as well as other countries considering data localisation mandates). A key part of these steps involves considerations on the way the governments should categorise data:

12.1 Considerations:

- What are the objectives of localisation?
- What are the potential spill-overs and risks of a localisation mandate?
- What are the existing alternatives to attain the same objectives?

12.2 Approach

- What data might be beneficial to store locally for ensuring national interest?
- What data could be mandated to stay within the borders of the country? What are the various models that can be adopted?

The report suggests that instead of imposing a generalised mandate, governments may wish to identify sectors or categories of data that may benefit most from local storage. The report also suggests that for all data not covered within the localisation mandate, countries should look to develop conditional pre-requisites for transfer of all kinds of data to any jurisdiction, such as the Latin American countries, or the EU.

It is difficult to find strong empirical evidence that the introduction of broad data localisation policies itself causes sustained growth in the local digital economy. Whilst data localisation can contribute to local jobs and investment, these gains may be offset by the many associated costs that may arise as a result of data localisation mandates. As noted by the Centre for Internet and Society, India, a study by Leviathan found that localisation laws could potentially increase costs of setting up servers in a country by 30-60%. The study found that a customer located in Brazil, would pay 54.65% less by using cloud servers outside Brazil, rather than requiring only Brazil-located cloud computing resources. Furthermore, studies found that splitting of datasets as a result of data localisation requirements might lead to the creation of vulnerable points, which is

compounded by the possibility of error when the prospect of mirroring is introduced. Together, these findings indicate that the costs associated with localization measures act as a likely disincentive for Foreign Direct Investment, which is critical for a growing digital economy.

The ability to move data and access information across borders is essential for businesses of all sizes, sectors, and geographies. A broad data localisation mandate risks cutting off South Africa from global flows of information and potentially have a negative impact on the country's digital transformation in that it would create barriers to trade, investment, and economic competitiveness. This may result in a reduction of digitally offered services where enterprises cannot comply with this requirement, there may also be fewer digital goods and services to choose from in the marketplace, and this may come at a higher cost with poorer quality leading to limitation on digital trade.

A balanced model involves the application of specific data handling or management requirements to narrowly identify data based on specific criteria, a government may determine that specific sectors or specific data that should be subject to data residency or localisation requirements. For example, Australia has legislated to require health data to be stored in Australia. Other than that, Australia does not have any other data localisation requirements for specific categories of data. However, when it comes to classified information, as with the UK, Australia takes a data residency approach and contractually enforces localisation requirements for certain classified data.

POLICY ISSUES ON COMPETITION (CHAPTER 10.7)

13 Overarching Comments

13.1 The proposed policy interventions outlined in Chapter 10.7 of the Draft Policy suggest that: (A) drastic regulatory intervention is necessary in the data and cloud computing sector; (B) competition law should be amended to create a level playing field in the digital sector; and (C) an open data strategy should be introduced for enhanced competition.

13.2 As background to these policy interventions, we note that the Draft Policy states that there is alleged market dominance and possible anti-competitive behaviour within the data and cloud computing environment in South Africa. In this regard, the Draft Policy has not presented any market analysis demonstrating the presence of dominant data and cloud computing businesses (or barriers to entry) in the South African marketplace which may necessitate regulatory intervention.

13.3 It is our view that for a regulator to intervene in the data and cloud computing environment, there has to be a market failure, for example, a service provider or technology company holding monopoly power or the existence of significant barriers to entry for new entrants. No examples of such activities have been presented in the Draft Policy and on this basis, we do not believe that the DCDT has demonstrated a sufficient basis for any regulatory interventions.

13.4 In addition to the current data and cloud computing environment, it is of concern that there has been no economic and/or market assessment in respect of the potential economic impact which the proposed policy interventions will have on the South African data and cloud computing sector. The decreasing price of cloud computing solutions combined with the wide availability and ease of obtaining data are among the factors that have fuelled the development of the digital economy in many countries and regions. As a starting point, any policy intervention should ensure that the economic development and growth activities envisaged by the Draft Policy would not be undermined by the proposed regulatory intervention. This is a critical instrument to estimate the impact on markets and to ensure that any regulatory initiatives are proportionate and constitute a minimal intervention.

13.5 We are of the view that any regulatory intervention in the data and cloud sector should focus on creating an environment that is conducive to the emergence of job opportunities. The combination of: (i) infrastructure liberalisation; (ii) technological innovation; and (iii) flexible service conditions, has led to job creation in a number of technology-centric countries. The Draft Policy should thus ensure favourable conditions in which technical progress can contribute to job creation and further the South African government's stated aim of harnessing the benefits of 4IR for economic growth and job creation.

14 <u>Specific Comments</u>

14.1 We note that the DCDT has largely followed the approach of the Competition Commission in its recent paper on the Digital Economy where it refers to the threats of big tech for new market entrants and the market power held by a few technology companies.

14.2 The Draft Policy has stated that, "existing legislative frameworks would need to be adapted to provide for competitive and contestable markets." The statements are somewhat surprising in light of the fact that there has been no evidence presented about the South African marketplace and whether there are material competition issues.

14.3 The Draft Policy then goes further to say that existing legislation and policies should be broadened to provide for: (i) consumer choice; (ii) market structure; (iii) switching costs; and (iv) lock-in effects. In this regard, the Draft Policy quotes the Digital Economy Paper and references the protection that is required for small businesses. We note that the DCDT focuses on the following aspects, namely: (i) data concentrations; (ii) market power; and (iii) first mover advantage, which we discuss further below.

14.4 *Data concentrations:*

14.4.1 The DCDT claims that the data and cloud computing market structure is dominated by a handful of large multinational companies. The alleged market dominance has not been substantiated in the Draft Policy and no information of the South African marketplace has been presented by the DCDT. Additionally, this characterization does not fully account for how local customers acquire cloud services. In South Africa and elsewhere, Global Cloud platforms work with a number of local partners, distributors, and resellers to bring cloud services to end customers. The preference is to work with these local companies, who in turn work with local customers, creating additional jobs and economic opportunity. For instance, a recent IDC study found that for every $1 of Google Cloud Products sold, partners generate $5.32 predominantly through their own offerings, but also through resale margin[1].

14.4.2 The Draft Policy then goes further to state that, "the concentration of data within this limited number of corporations poses a risk as it limits possibilities for the extraction of public value of data." In addition, the DCDT has argued that the alleged lack of market competition has provided consumers with few alternative choices for the protection of privacy, and they claim that there will likely be no other choices in the future. To the first point on market competition, it is important to note that multiple cloud providers currently invest and operate in South Africa, including multinational corporations and a number of local hosting providers. Second, regarding privacy protection, it is critical to note that with Cloud services, customers own their data, not the Cloud provider. Cloud services process customer data only according to customer agreements.

14.4.3 The Draft Policy claims that cloud providers do not use open source standards, which

[1] IDC, Partner Opportunity in a Cloud World How Partners Are Winning in the Google Cloud Economy, August 2020. https://idcdocserv.com/US46702120BROI

presents difficulties for smaller organisations to move between public and private cloud platforms. This does not take into account open cloud solutions that provide organizations with choice, flexibility, and agility in their technology for instance Kubernetes and TensorFlow, which have enabled innovation and competition across the cloud industry. In addition to open source contributions, many Cloud providers allow organizations to operate across different types of architecture, including on-premises data centres, hybrid cloud deployments, and multicloud environments. These solutions give customers flexibility in their use of cloud services, as well as the autonomy to migrate their data safely and seamlessly if needed.

14.4.4 The DCDT also makes a number of unsubstantiated arguments about the South African marketplace, which includes that: (i) there is no equal opportunity for new entrants to participate in the market; (ii) new entrants do not have the financial means to own and operate IT systems (as found in large organizations); and (iii) new entrants do not have access to data storage facilities, such as cloud or other data centres.

14.5 *Market* Power

The Draft Policy quotes the Competition Commission on its position on market power (within the digital sector) and the issues around vertical integration. The extracted section used by the DCDT also refers to the fact that, "Online resale price maintenance has also been investigated in European cases resulting in decisions against manufacturers of consumer electronics." Similar to the issues highlighted above, the DCDT has not made any independent finding on the current position of the South African data and cloud computing market.

14.6 *First Mover Advantage*

The DCDT has stated that, "*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.*"

15 Concerns

15.1 The Draft Policy's general statements about big data's propensity to raise barriers to entry is misleading. Whether big data raises or lowers barriers to entry also depends on the nature and use of the data and the availability of alternative data sources. Its value is also highly dependent on the availability of advanced technology and digital skills within the population to harness insights from said data.

15.2 The mere fact that a particular dataset (including a valuable one) is unique and non-replicable does not imply that competitors necessarily need access to the same or even similar data to compete in the market.

15.3 Further, the inference that data-related barriers to entry translate into market power is without merit. The nature of a data holder's market power depends on the competitive structure of the market in which it is active. Even if the need for big data does create a barrier to entry, it does not follow that a company holding such data has market power or a dominant position.

15.4 We are of the view that data is a product of research, innovation and investment in analytics that ultimately provides firms with a comparative advantage. Furthermore, given that data varies in its value and usefulness (which is extracted through use of proprietary algorithms), it cannot be guaranteed that the data held by one entity is essential for the entry or expansion of another.

15.5 As a recurring theme throughout the Draft Policy, we are concerned that no economic and/or financial data has been presented in respect of the South African marketplace and that the DCDT has not provided any evidence of dominance and/or anti-competitive behaviour within the data and cloud environment.

15.6 We are also concerned by the statement that the academic concept of 'FAIR', which has not been analysed for the commercial sector, would be followed within the South African competition landscape. There is no economic theory that justifies the introduction of FAIR principles into South African competition law, and we are concerned by the regulatory direction being proposed by the DCDT. Similarly, the DCDT's proposal that an open data strategy be introduced (for the private sector) is far reaching and would have a material impact on the commercial use of data and associated data

analytics that are conducted by technology companies.

15.7 The intended focus of the DCDT that there will be "disruption" throughout various sectors (by means of regulatory intervention) is also concerning, as there has been no indication of the market failures that the DCDT is trying to address.

15.8 As a general comment, we wish to note that a regulatory environment that is not fit for purpose could create problems for investing in South Africa and the technology industry at large. We are concerned that the proposed competition changes may lead to a number of unintended consequences such as stifling innovation, impeding job opportunities and deterring potential investment.

15.9 In addition, we have noted that the proposed policy interventions potentially create competition concerns in and of themselves. Specifically:

15.9.1 Concentration risk in the HPCDP including:

- uncertainty regarding Government relationships with the service providers
- Allowing for sub-outsourcing,
- multiple outsourcings to the same service provider
- outsourcing critical or important functions to a limited number of service providers

15.9.2 A key area for concentration risk is with SITA as the owner of the envisaged HPCDPC. How will the Government relationships with service providers be monitored? Key areas to monitor:

- Allowing for sub-outsourcing (e.g. building of the HPCDPC)
- multiple outsourcings to the same service provider
- outsourcing critical or important functions to a limited number of service providers

15.9.3 Policy interventions required on reducing concentration risk in the HPCDPC include defining how concentration risk will be measured and monitored including key metrics such as (a) concentration of spend; (b) concentration of non-containerized workloads on a single CSP; and (c) concentration of most critical technology services.

16 Recommendations

16.1 The regulatory policy for data and cloud computing services in South Africa should be internationally harmonised and fit for purpose.

16.2 The proposals by the DCDT to introduce: (i) FAIR principles (within the competition framework); (ii) an open data strategy; and (iii) disrupt the market, are not in accordance with international best practice and will inevitably stifle innovation and job creation in an already ailing economy.

16.3 A clear regulatory framework should be developed which focuses on the key regulatory objectives of the government, and this should be achieved by using a risk-based, measured approach. It is recommended that the DTDC follow international best practice and any regulatory framework for the data and cloud computing sector focus on: (i) economic growth and expansion of the data and cloud computing sector; (ii) the establishment of legal certainty across the ecosystem, including alignment with international standards; (iii) innovation; (iv) supporting user choice; and (v) accommodating new technologies.

16.4 We do not believe that there is a legal basis to impose far reaching competition law changes where the regulator has not been able to demonstrate any market failures as a result of the presence of data and cloud computing services in the technology market. As addressed earlier, it is our view that a regulator should only intervene in a marketplace if there has been a market failure of some sort.

16.5 Finally, to the extent that access to data could be found to raise competition concerns, a potential alternative may be to focus on sharing aggregated datasets, which can have wide-ranging uses and applications, but which avoids jeopardising privacy and innovation.

POLICY ON SKILLS AND CAPACITY DEVELOPMENT (CHAPTER 10.8)

To contribute to the digital economy which continues to grow exponentially, driven by cloud computing technologies that enable collection, analysis, and synthesising of massive amounts of digital data, we propose that the DCDT focuses on implementation of the policy interventions outlined in the Draft Policy. The Working Group was largely in agreement with the proposed interventions.

17 Defining Skills

The Draft Policy does not indicate the skills that need to be developed to equip resources to work in the data and cloud environment.

17.1 Proposed solution:

The areas that requires skills need to be established first. The key cloud offerings that are forecasted to be the biggest trends and an opportunity for government are:

- Infrastructure as a service (IAAS);
- Software as a service (SAAS);
- Platform as a service (PAAS).

The Working Group assessed the relevant skills associated with the above areas and propose that the DCDT incorporates them into the Draft Policy which include:

- Collaboration between the Department of Basic Education to introduce basic programming languages at primary school level
- Collaboration between Department of Higher Education as well TVET collages to fund computer science students. According to recruiters within the sub-committee graduates with this background perform exceptionally well
- MICTSETA collaboration on advanced specialist skills. These are listed below. These are offered as certificates by IT learning and development. They are often globally developed programs that can aligned to local MICT SETA unit standard. There needs to be a concerted effort to approve the certification of these programs by MICTSETA. Skills are
    - Data analysis
    - Cloud platform
    - Containarisation
    - Data science

18 Proposed Interventions to address skills development

The development of scarce data skills will contribute to the increase of job creation opportunities for

unemployed youth and adults, mentorship to Non-profit organisations as well as provide Subject Matter expertise to government institutions such as the DCDT.

18.1 *Issue in Draft Policy*: The Draft Policy fails to propose a model or detail on how this would happen but acknowledges the need to develop skills in the space

18.2 *Proposed solution*: The Working Group is of the view that government alone cannot develop skills without collaboration with multiple stakeholders, both local and multinational. Essentially there needs to be an establishment of an eco-system where government acts a convener. The model in which the eco system would be based on is outlined below.

- **Demand-led skilling**: Equip NEETS (Not in Education, Employment, or Training) with the above mentioned data and cloud skills to get a job or build a business in a short space of time. As the demand for skills will change rapidly from year to year. The government needs private industry to advise and help execute on skills. This could be achieved through multinational organisations that are at the face of cutting-edge developments. many of the key digital skills are novel, they are not yet offered by Higher Education Institutions
- **Short term programmes that are MICTSETA aligned** Determine ongoing initiatives and programmes such as
    - CODEX
    - Skills to Succeed through Johannesburg Software Engineering College (linked to Wits)
    - UCT data analysts programme
    - CSI programmes through NGO

- Nemisa linked to Microsoft
- JCSE (Johannesburg College of Software Engineering) linked to Accenture
- Mentec linked to Accenture

- **Employment and entrepreneurship partnerships**: Increase our focus on the successful transition from skill-building programs to sustainable jobs and businesses, and improve our collective ability to measure and report on these outcomes:
  - To ensure transfer of wealth and socio economic development, the provision of cloud and data services needs to include SME service providers.
  - Through a Joint venture arrangement with multinational ICT firms is needed. The condition such as percentage ownership of contracts should be outlines
  - This will ensure transfer of knowledge as well as socio-economic development

- **Collaboration for systemic change**: Bring together organizations across sectors and multinational to create large-scale, lasting solutions aimed at closing skills gaps within the future data and cloud space.
- In order to expand the data and cloud programme and to expand government reach there needs to be participation and involvement into other industries
- An index to identify key industries of focus can be developed
  - The index would identify: Financial Services, Wholesale & Retail, ICT and Government as the most attractive for future skills development initiatives
  - After taking into account additional screening factors, identified industries would need to fall within government's priority sectors for future economic development and employment growth
  - These sectors have however been listed under "Priority Areas" in this document, and the Working Group recommends that they be addressed in the second phase of the research

POLICY ON RESEARCH, INNOVATION AND RELATED HUMAN CAPITAL DEVELOPMENT (CHAPTER 10.9)

The Working Group was largely in agreement with the proposed interventions.

19 Issue in Draft Policy: The Draft Policy does not indicate the institutions or mechanisms that can be used to conduct R&D on big data and cloud space.

20 Proposed solution: There are several institutions that conduct detailed research on Big data and cloud trends, skills, and ICT in general. They are well versed and keep abreast of developments locally and globally that can assist the DCDT in implementing the strategic objectives. It's important for the institutions to conduct ongoing research due to the rapidly changing nature of this industry. The institutions need to work in an agile manner.

CONCLUSION

21 The DCA and the Working Group thank the Department for the opportunity to engage on the Draft Policy and we re-iterate our desire to be included in any further consultations / workshops or public hearings to be held in the further development of this Draft Policy