

1 June 2021

The Director- General, Department of Communications and Digital Technologies

For Attention: Ms. C Lesufi, Director General, Telecommunications Policy

DataCloudpolicy@dtps.gov.za**SUBMISSIONS ON THE PROPOSED NATIONAL DATA AND CLOUD POLICY**

1. The Internet Service Providers' Association of South Africa (**ISPA**) refers to the Proposed National Data and Cloud Policy ("**the Draft Policy**") published for comment on 1 April 2021 by the Minister of Communications and Digital Technologies ("**the Minister**") and sets out its submissions below.
2. ISPA supports the development of policy which 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. ISPA welcomes in particular the emphasis in the Draft Policy on openness: open data, open source and interoperability.
3. ISPA members are critical players in enabling the use of cloud services and primary users of the services of data centres and exchange points and as such have an interest in the finalisation of the Draft Policy.

Scope

4. ISPA understands that the DCDT is taking a leading role within Government in promoting e-Government and the adoption of the recommendations set out in the Report of the Presidential Commission on the Fourth Industrial Revolution ("**the PC4IR Report**").
5. Notwithstanding the need for such leadership, the scope of the Draft Policy appears overly broad, while encroaching on what ISPA understands to be matters already subject to regulatory and/or institutional frameworks.
 - 5.1. There is an existing legal framework for the declaration of infrastructure as being "critical infrastructure" under the Protection of Critical Infrastructure Act 8 of 2019.
 - 5.2. Data protection is now comprehensively provided for under the Protection of Personal Information Act 4 of 2013 and governed by an independent regulator in the form of the Information Regulator. The Information Regulator also oversees the implementation of the Promotion of Access to Information Act 2 of 2000.

- 5.3. Cybercrime is comprehensively provided for in the recently-enacted Cybercrimes Act 19 of 2020.
- 5.4. Transformation and skills transfer obligations – including those applicable to foreign companies investing in South Africa - are provided for under the BBBEE framework overseen by the Department of Trade, Industry and Competition (“**the DTIC**”).
- 5.5. Competition issues are governed by the recently amended Competition Act and the Competition Commission has adopted an activist role in addressing competition in the online environment.
6. ISPA has no difficulty with restating policy, law and regulation falling outside of the immediate area of competence of the DCDT where this is necessary to reflect the transversal approach which policy of this nature must adopt. However, it is not clear on what basis the Draft Policy seeks to vary existing policy and legislation.
 - 6.1. For example: the Draft Policy sets out an intent to undertake a review of “the existing regulatory authorities mandates with a view to establishing a single data regulator, reporting to the Minister of Communications and Digital Technologies”.
 - 6.2. ISPA understands that there already is a single data regulator – the Information Regulator very recently established under the POPIA – reporting to the Minister of Justice and Correctional Service.
7. Further - in a period of budget austerity - the DCDT needs to be careful about taking on too much (with the associated risk of achieving too little).

“National critical information infrastructure”

8. The Draft Policy sets out the following definition:

“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.
9. The Draft Policy further states:

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.¹

10. ISPA notes further that the “Policy, Legislative and Regulatory Landscape” set out in section 2 of the Draft Policy does not reference the Critical Infrastructure Protection Act 8 of 2019, which deals comprehensively with the concept of “critical infrastructure” as set out in the Draft Policy. This Act is in the process of being implemented.
11. ISPA submits that the Draft Policy must be aligned with and should explicitly reference the Critical Infrastructure Protection Act. It should recognise that the process for determining what is to be declared as “critical infrastructure” is set out in the Critical Infrastructure Protection Act.
12. The Draft Policy appears to contemplate that all digital infrastructure is “critical” simply on the basis of the importance of digital infrastructure in South Africa. ISPA submits that this is not a competent determination.

Proposed Policy on Digital Infrastructure:

13. ISPA supports the consolidation of government ICT infrastructure assets, capacity and services as a practical and overdue step.
14. ISPA calls on the Minister to ensure that the scope of operation of the State Digital Infrastructure Company (SDIC) is clearly defined.
15. ISPA supports recognition of the need to allow data centres a degree of flexibility in meeting their power requirements given ESKOM supply challenges and requests that the DCDT involve the data centre industry in formulating the necessary approaches to the relevant government stakeholders.
16. ISPA further supports considered measures designed to incentive investment into digital infrastructure such as data centres and electronic communications networks.
 - 16.1. Any such measures must be aligned with the broader work of the DTIC and the various infrastructure investment initiatives housed within the Presidency. This would include requirements relating to digital technology transfer to ensure the capture of benefits and gains from Foreign Direct Investment (FDI).

¹ @ p17. As an aside: ISPA is not at all certain that it is either correct or desirable to refer to “data as infrastructure” or people being “national critical information infrastructure”.

- 16.2. In considering utilizing the framework for Special Economic Zones (SEZs), the DCDT should note that the location of certain categories of electronic communications infrastructure is dictated by practical and market requirements. Data centres, for example, are typically located where there is a confluence of major fibre networks as well as sufficient power supply and proximity to the data centre's customers.
- 16.3. Measures designed to incentivize investment in data centre infrastructure should therefore not be linked to the concept of geographically dispersed ICT SEZs.
- 16.4. ISPA notes that the Dube TradePort SEZ has many of the features of the proposed ICT SEZ and the Dube TradePort Corporation is an active provider of licensed services.
17. ISPA members regard the rapid evolution of the local data centre industry and the emergence of carrier-neutral facilities for peering and interconnection as one of the most important factors in promoting competition and driving down the cost to communicate in South Africa.
18. Although it is now taken for granted, a highly competitive and world-class data centre industry has underpinned open access models, kept traffic local and enabled local networks to convey the huge amount of video and other rich content media consumed by South Africans.
19. This is borne out by the decisions of most major cloud providers to utilise local data centre providers, while the decision of Amazon to build its own dedicated facility speaks directly to the future potential of the local and African market and the suitability of South Africa to serve that market.
20. Undersea cable connectivity serving South Africa – once a bottleneck – has increased exponentially and will continue to do so while also enabling the provision of cloud services to other African countries.
21. ISPA therefore requests that any policy intervention targeting data centres carefully consider the impact on what is already a continent-leading industry as well as the potential consequences for the cost to communicate in South Africa. South Africa is competing with jurisdictions such as Kenya and Rwanda for investment into data centre infrastructure and cloud services: measures which introduce policy uncertainty or otherwise disincentivise investment must be avoided.

Proposed Policy on Access to Data and Cloud Services

22. As noted above, ISPA strongly supports the clear emphasis in the Draft Policy on open data, open access, data sharing and interoperability.

23. ISPA suggests that the Proposed Policy make explicit the need to align with international best practise, including the use of ISO and other relevant standards, to ensure that there is inter-country interoperability.

Proposed Policy on Competition Issues

24. ISPA's view is that competition in the provision of data centres services is generally effective.
25. ISPA suggests that competition issues should – to the greatest extent possible – be left within the competence of the existing competition law institutional framework.

Proposed Policy on Cybersecurity

26. ISPA welcomes an explicit statement of support for the Cybersecurity Hub and a commitment to ensuring that it is capacitated to perform its function. Cybersecurity requires close collaboration between the public and private sector and the Cybersecurity Hub is important in facilitating this.
27. ISPA looks forward to continuing working with the DCDT and the Hub to implement the proposed policy provisions.

Conclusion

28. ISPA extends its gratitude to the Department for its consideration of these submissions.

Regards

ISPA