

ENDCODE UPDATE:

The below insight is a non-commercial gratuitous contribution for the public good. Please note that our submission below does not constitute an in-depth analysis. This piece may be used as the basis of further in-depth analysis.

Draft National Data and Cloud Policy: The Key Proposals

1) Introduction

On 1 April 2021, the Minister for Communications and Digital Technologies published the proposed [National Data and Cloud Policy](#), inviting written submissions within 30 working days of the date of publication (1 April 2021). The proposed Policy is contextualised against the opportunities presented by the Fourth Industrial Revolution (4IR) and the need to realise the benefits of the digital economy. According to the proposed Policy, the adoption of strategies and interventions to exploit opportunities presented by data and cloud computing are needed to enable the development of various applications, services and technologies. There is a broad recognition that initial ICT policy and regulation did not appreciate the potential of data in the digital economy whilst recent policies (and strategies) and regulatory frameworks (for privacy and cybersecurity) have a better appreciation of the range of regulatory considerations. The draft Policy assesses however that a policy to guide “localised data acquisition, ownership, storage, use and analytics” is lacking presenting a “threat to both national security and social and economic growth”.

The rationale for the Policy ultimately, is to strengthen the capacity of the State to deliver services to its citizens, ensure informed policy development in the context of data analytics, promote data sovereignty and the security of data.

2) A snapshot of specific proposed intervention within targeted policy and regulatory areas

- **Digital Infrastructure:**
 - ICT infrastructure framework to support key economic sectors for economic growth through provision of connectivity, data centres, computing and data processing and storage facilities.
 - Digital infrastructure of “critical scale” be declared a national strategic asset and data centres hosting critical cloud computing declared critical information infrastructure.
 - Establishing a High-performance Computing and Data Processing Centre (HPCDP) that consolidates public funded data centres.
 - Establishment and operationalisation of a Digital Transformation Centre that converges and coordinates various digital transformation objectives.
 - Establishing Digital Economic Zones to support local and foreign investment in data and cloud infrastructure.

- **Access to Data and Cloud Services:**
 - Formulation of a National Open Data Strategy to address sharing, interoperability, ownership, data sovereignty, economic rights, integrity and quality of data and give effect to open government action plans and manual.
 - Provision of universal access to non-sensitive data in the HPCDP (subject to regulation)Developing a model for localised data banks in the HPCDP to enable data analytics Sector level data classification guidelines informed by State Security classifications

- **Data Protection:**
 - Review of ECTA to align it with cybersecurity policy and legislation;
 - Data stored in the HPCDP to conform with State Security prescribed security measures;
 - Review of measures to protect sensitive data in the digital economy;
 - Use of private cloud for sensitive data in line with government data protection frameworks including PAIA; and

- Regulatory institutions to develop regulatory and monitoring frameworks to give effect to data residency.
- **Localisation and Cross Border Transfers:**
 - Data classified as critical information infrastructure to be processed and stored within South Africa.
 - Cross border transfers subject to POPIA, the Constitution and international best practice and a copy of the data to be stored in SA for the purposes of law enforcement.
 - For ownership and control: Data generated in SA is to be the property of South Africa with government as a trustee for all government data generated in SA.
- **Cybersecurity:**
 - National Cybersecurity Policy Framework to be reviewed for responsiveness to threats and risks of digitisation.
 - Cybersecurity Hub to be capacitated to respond to threats and risks of digitisation.
- **Governance and Institutional Mechanisms:**
 - Establishing an Advisory Council to advise on various matters including data management standards, regulatory frameworks for data and cloud services, policies on an AI code of ethics.
 - Review of existing regulatory authorities mandates to establish a single regulator reporting to the Minister of Communications and Digital Technologies.
 - The Department of Public Service and Administration to develop norms and standards on data for the public service.
- **Competition:**
 - A Competition Policy to enable creation of, access to and capturing of value from data and cloud services.
 - Review of legislation to provide for competitive and contestable markets.
 - Policies and legislation to be broadened to consider, consumer choice, market structure, switching costs and lock-in effects.

- **Data Concentrations:**

- Measures to address the concentration of data within a limited number of multinational companies that limit the possibilities for the extraction of public value from data.
- Various measures to address Skills and Capacity Development and Research, Innovation and Human Capital Development policy areas.