Ecommerce Forum South Africa

Submission to the Department of Communications and Digital Technologies on the Draft National Policy on Data and Cloud

The Ecommerce Forum of South Africa[1] welcomes the opportunity to respond to the Draft National Policy on Data and Cloud issued by the Department of Communications and Digital Technologies (DCDT) on 1 April 2021.

The Draft Policy raises key policy issues which government should address. As the draft says *"… the advent of the Fourth Industrial Revolution (4IR) and its related technologies presents an opportunity to address the social and economic challenges characterizing the South African economy".*[2] The COVID pandemic has contributed to the rapid development of the digital economy in South Africa, on the African continent, and globally. Wise regulators will be taking the opportunity to revisit out of date regulations and policies to craft new approaches and new solutions to protect consumers and promote business.

EFSA was therefore encouraged to read that the DCDT recognises the need to strengthen South Africa's cyber security environment; to provide means to address cybercrimes; to consider the important role intellectual property plays; and to review the role of the relevant regulators in the data and cloud ecosystem. EFSA looks forward to the DCDT's further proposals on these key issues. However, the Draft Policy does not mention the Cybercrimes Bill, which was passed by Parliament in December 2020 and which is currently awaiting signature from the President, save to propose that cybercrime legislation will provide for enforcement and sanctions against cybercrimes. This reference may need to be reviewed and incorporated accordingly.

We appreciate the rationale provided for the Data and Cloud Policy including the acceleration interventions aimed at unlocking investment opportunities, ensuring inclusive economic growth, education, and job creation. The Paper also outlines the need to intensify South Africa's global presence and competitive advantage and grow small and medium sized firms. Digitalision and its associated benefits can significantly support the growth and cross border expansion opportunities of SMEs.

The issue of the digital divide in South Africa is also referred to in the Paper. EFSA has frequently expressed its concern that the digital divide in the RSA must be addressed as a matter of urgency to permit rural SMEs, women, youth, and the disadvantaged to enter the digital economy and benefit from digital commerce. Three government policies are required

[1] The Ecommerce Forum South Africa (EFSA) is a not-for-profit membership driven organisation founded in 2016 and is the national chapter of the pan-African Ecommerce Forum (EFA).
[2] The DCDT's Draft National Policy on Data and Cloud ("the Paper"), 1 April 2021, page 3.

in order to break through the digital divide – first, continue to reduce the cost of data (the cost of data in the RSA remains the highest of all the digitally active countries on the continent); second, encourage the establishment of telecommunications relay towers to reach as high a percentage of the population as possible; third, encourage the move from 2G phones by promoting low cost 3G and 4G phones, with the vision of affordable, accessible 5G phones in the future.

A National Policy on Data and Cloud is of little concern to those excluded by the digital divide.

The EFSA strongly supports the Paper's statements that - "*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[s]. Digital platforms create scalable implementations through large-scale ecosystems which enable collaboration with other ecosystem partners and are easily orchestrated by the digital platforms." "Investment in infrastructure needs to be supported by clear protocols for information security, cyber security and a data governance framework supporting open data principles."*[3] We note that there needs to be a clear policy directive on the change management process that runs in tandem with any expansion within the digital domain, especially within the realm of customs and other regulatory agencies, in particular with regard to free trade across the African continent.

EFSA has stressed in other submissions to government, the need for more private and public investment in the digital economy, and the benefits of economies of scale which will be achieved by increasing the market. EFSA is the national chapter of the pan-African Ecommerce Forum Africa which was set up to encourage the development of the digital commerce throughout the African Free Trade Area (AfCFTA). The greater the volume of intra-Africa trade, the more opportunities will be presented to scale South African businesses and re-industrialize RSA.

EFSA regrets that the Paper ignores the role (and responsibility) as well as the leadership opportunity of the RSA in the AfCFTA. We had hoped that this would be a central aspect of any future-proofed digital policy. We will return to this point later.

The Paper also stresses the need for more skills development and education of the citizen on the digital economy. EFSA fully supports this. Teaching the aspects of the digital economy (not just on data and cloud) from secondary school onwards is essential. This will require equipping rural schools with the applicable technology and infrastructure to enable this. School children will be able to explore career possibilities and will help their parents appreciate the new ICT developments. Such educational initiatives should also be focused within the education sector itself to ensure a higher maturity of cyber-safety within South African schools. It is critical that any training and expertise proposed to school children must also be coupled with increasing the level of cybersecurity and data protection maturity in

[3] Ibid, pages 4 and 5

P O Box 1753, Jukskei Park, Gauteng 2153 RSA Tel: +27 11 704-0937 Email: info@ecomafrica.org

South African schools to enable a culture of understanding on the benefits and risks associated to the digital economy. [4]

As the government has recognised, tertiary level training will equip young citizens and prepare them for the future; and university research will continue to help position South Africa as a leader in technology-driven solutions (for example in fintech).

We therefore strongly recommend that the Policy strengthens its recommendations on skills and education,[5] as well as resourcing of schools to enable this.

The main thrust of the Paper, however, addresses data localisation and the DCDT's proposals to share data with the private sector with the intention to benefit both the public and private sector. This proposal needs to be broken down into three parts – first, the benefits and disadvantages of data localisation: second, the protection of privacy, and, finally, the role of South Africa within the AfCFTA.

What is Cloud Computing?

Before considering the pros and cons on the Paper's proposals, we respectfully suggest that it would be useful to define the 'cloud'. The recommendations of the DCDT's Paper are mainly addressed to **cloud storage**.

There are many different types of cloud computing. The widely accepted definition of cloud computing is an ICT sourcing and delivery model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It is not a new technology, but a service delivery model.

Cloud storage in most cases uses multiple separate services to store data. The more servers and other services available, the more likely that the system will provide a secure environment for data stored within it. The most secure storage services divide the totality of the data into small packages which by themselves are meaningless until brought together by the client/owner and are therefore provided with a much more secure system to protect against hacking/cybercrime. [6]

Data Localisation

[4] See for example https://www.mdpi.com/2078-2489/11/10/471/pdf
[5] Ibid. Recommendations 10.8.2 and 10.8.3 , page 35.
[6] Please note that most data placed in cloud storage services is owned entirely by the customer. Therefore, the statement that *"… the data generated in Africa and South Africa is mostly stored in foreign lands and, where stored locally, is owned by international technology giant companies*" should be amended to reflect actual practice. This statement seemingly contradicts the point on data portability made on p 33. We respectfully suggest that the government's own experts are consulted to clarify the ownership of data carried in cloud storage - https://www.chpc.ac.za/

P O Box 1753, Jukskei Park, Gauteng 2153 RSA Tel: +27 11 704-0937 Email: info@ecomafrica.org

Data localisation policy requires that data is stored on a device or devices physically present within the borders of the jurisdiction where the data is generated.

The DCDT Paper would allow data generated in the RSA to be stored outside RSA, however a copy of any data generated within RSA will have to remain in cloud storage in the RSA.

Commentators have noted that data localisation requirements serve multiple governance and monitoring purposes, such as:

- Enhanced data privacy and sovereignty from foreign surveillance;
- Greater efficiency in the data monitoring, owing to unfettered supervisory access of data;
- Increased regulatory control since national governments and regulators can more effectively enforce laws within their jurisdictions;
- Greater accountability in respect of end-use of data.

Notwithstanding these advantages, serious costs and trade-offs need to be considered in respect of data localisation. Experts and researchers of data localisation have noted that the policy threatens to undermine many of the efficiencies and economic opportunities of the digital economy and that other mechanisms can be employed which offer the same benefits, notably in respect of enhanced privacy, security, and digital opportunity.[7]

The International Institute of Finance (IIF) in a 2020 report[8] noted that the principal shortcomings, challenges, and disadvantages of data localisation are that it:

- Reduces connections to digital trade, negatively impacts on economic growth and development, and reduces ease of doing business in countries that apply data localisation policies.
- Weakens fraud prevention, and cyber security defence.
- Slows scientific discovery, health diagnostics, and telemedicine.
- Reduces access to the best and newest cloud-based software, technology, and future cloud-first technologies such as quantum computing.
- Undermines cost-effectiveness of cloud-based computing.
- Blocks innovation and competition through reducing access to the public cloud, which is a key for the development of fintech and other innovative start-ups by providing low entry costs, scalable platforms, and embedded services.
- Reduces fast payments, low-cost remittances, and other services that individuals, households, and small businesses (such as ecommerce shops) need to function in the digital economy.

[7] See *inter alia* – https://researchictafrica.net/2021/05/10/watch-what-are-the-implications-of-south-africas-draft-national-data-and-cloud-policy/; https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf March 2019; https://www.deltapartnersgroup.com/data-localisation-information-protection-balkanisation-internet; The Global Economic Governance, South Africa and data flows, how to fully exploit the potential of the digital economy, Martina F Ferracane, April 2018; and the recent work of the Internet & Jurisdiction Policy Network, www.internetjurisdiction.net .

[8] Data Localization: Costs, Tradeoffs, and Impacts Across the Economy December 22, 2020

P O Box 1753, Jukskei Park, Gauteng 2153 RSA Tel: +27 11 704-0937 Email: info@ecomafrica.org

- Weakens resilience of the financial system. The ability to have seamless failover redundancy systems and storage outside geographical borders improves cybersecurity.
- Adds hard costs which redundant local data infrastructure will create.

EFSA respectfully suggests that these disadvantages will lead to barriers to the use of cloud computing services to store data and process transactions in the RSA. This negatively affects both local and foreign firms, especially start-ups, governments, and, ultimately, consumers. Moreover, data localisation is a barrier to the use of integrated, secure, and efficient payment systems worldwide, creates barriers to competition, and increases costs to all as well as the leadership opportunity for South Africa, and therefore has the end effect of working against central policy objectives outlined in the DCDT's paper.

In respect to the effective development of ecommerce in the RSA, EFSA would like to highlight in particular -

1) Cross border banking/payments - data is required and transferred at every step of a transaction in cross-border e-payment services. Depending on how the data localisation rules are applied, these can become a significant legal barrier to both market entry and operations for e-payment service providers.[9] Cross-border data flows are required for e-payments not just in transnational transactions but also often in purely domestic transactions. This point is key to the future development of ecommerce in SA and Africa.

2) Data localisation policies undermine trade and economic growth because they reduce connections to digital trade and create adverse impact on economic growth and development. The OECD has pointed out that digitization is linked to enhanced trade openness by providing opportunities for ecommerce and e-government services which facilitate enhanced trade in services and goods. We will consider this point further below.

3) Data localisation undermines fraud prevention and cybersecurity best practices. The growing sophistication and complexities associated with technological advancement require the continuous evolution of cyber defence solutions. Public cloud service providers and cloud-based cyber security firms have provided cybersecurity solutions and ensured that cloud computing have failover redundancy storage inside and outside geographical or time zones. This allows data to be instantly moved between centres in situations of cyber-breaches and other forms of attack. Data localisation requirements undermine these solutions. Storing all data in one geographical region compromises data security and exposes the data to targeted cyber-attacks. A recent

[9] E-payment systems rely on blockchain systems, which in turn operate by accessing the Internet of Things (IoT). If access to the IoT is limited, blockchain will not function as effectively, and this will adversely affect the effectiveness of e-payments.

P O Box 1753, Jukskei Park, Gauteng 2153 RSA Tel: +27 11 704-0937 Email: info@ecomafrica.org

example: - Brazil's national government database which applies data localisation was recently hacked with the loss of over 220 million data sets.[10]

4) Countries that follow data localisation typically score low on the digital trade index. The higher the rate of digital trade restrictiveness, the lower the ranking of a nation's ease of doing business[11]. Those countries that have applied data localisation policies, such as China, Russia, India, Vietnam, and Indonesia, do not score high in respect of digital trade. A data localisation strategy, if enforced, may discourage international companies from locating in RSA and encourage South African digital economy companies to relocate out of the RSA. It is also important to point out that countries such as Russia and India have a significantly larger population already active online compared to South Africa. This means that the incentive for companies to establish or co-operate with such strategies posed under their respective data localization policies is significantly higher – this observation would be different if the Government takes into account the member states of the AfCFTA and the population across the African continent.

5) Data localisation stifles innovation. SMEs and startups benefit from the low cost of public cloud services. This cost efficiency allows those enterprises to utilize research, development, and innovation. In contrast, the application of data localisation undermines the cost efficiencies of cloud computing as the duplication of infrastructure and fragmented compliance standards are required. These are expensive and necessitate a notable financial outlay for small businesses. There are also associated costs concerning anti-fraud monitoring and the implementation of other compliance measures. These large outlays, coupled with the reduced access to resources offered by the public cloud, adversely impact the financial sustainability and longevity of startups and SMEs.
   According to a study by the World Bank (2021), The burden associated with mandatory localisation requirements impacts more on developing economies and their enterprises given the high cost of investment in infrastructure. In larger economies with significant domestic markets, localisation policies may be used to protect domestic infant industries from globally dominant competitors - this however has implications for competition policy.

Participation and integration in global value chains and the importance of improving access to global data flows have been highlighted by the COVID pandemic. One of the principal lessons learnt was the importance of integrating into digital markets; data localisation measures however erode the benefits of digital market integration.

[10] https://www.lexology.com/library/detail.aspx?g=f8cba4de-b585-4716-8684-9cb7cdf71024#:~:text=During%20January%202021%2C%20Brazil%20experienced,number%20of%20inhabitants%20in%20Brazil.

[11] See the OECD Digital Services Trade Restrictiveness Index Simulator and the Digital Trade Restrictiveness Index of the European Centre for International Political Economy

P O Box 1753, Jukskei Park, Gauteng 2153 RSA Tel: +27 11 704-0937 Email: info@ecomafrica.org

EFSA notes that national localisation requirements may be applied to selected types of data, such as government generated data, health data or financial data.[12] These rules usually permit cross-border transfers with conditions (for example, that the data is stored, processed, or backed up in the original jurisdiction - as proposed in the Paper). There are significant costs associated with data management in this respect, which can result in the disruption of cross-border business models (World Bank, 2021).

EFSA notes that the DCDT Draft National Policy on Data and Cloud does not propose the selective application of the data localisation regulation. Business must therefore accept that the intension is for data localisation rules to apply to **all** data, including sensitive data,[13] generated within South Africa.

The Protection of Personal Data ('data privacy').

The Paper points out that *"data is the new oil",* [14] however, EFSA humbly suggests that there are two very different issues that are being addressed in the Paper – first, personal data, and second non-personal information/data. Although broadly recognised in the definitions in the Paper, these two forms of data become increasingly confused in the Paper.

The Paper recognises the Protection of Personal Information Act (POPIA), which it states is one of the policy issues on which the Paper's policies are based. The Paper lists six (of the seven) universal personal data protection principles, which are also enshrined in the POPIA. However, the Paper goes on to state that "*The development of this policy and legislation [on Data Protection] did not take into consideration the context of the digital economy where data is the key driver of societal and economic development.*"[15] On the basis of this point, the Paper appears to challenge the effectiveness and currency of the POPIA in a number of ways in order to argue that the State should have access to some elements of personal data processed by private entities.

The privacy of personal data, which in the POPIA also includes an element of company (juristic person) data, is intended to prevent the unauthorized access, misuse/abuse, or

[12] National/regional examples include: - the EU's GDPR and Australia prohibit the overseas transfer of personal health data with some exceptions; Russia, Turkey and Korea apply localisation to financial data (with exception of financial data necessary for cross-border payments). It is important to note that the definition of "financial data" or "transaction data" has caused considerable confusion with guidance being requested by the impacted industries. A thorough understanding, explanation and impact on such requirements is required before being considered in South Africa. This confusion regarding localisation naturally extends to crypto-currencies due to nature of distributed ledgers (blockchain) used. An example is the Supreme Court of India case which set aside the Reserve Bank of India's circular banning cryptocurrency in March 2020: https://inc42.com/buzz/one-year-after-sc-order-indian-banks-again-wary-of-crypto-trades/ . In China, there are mandatory localisation requirements in respect of "critical information infrastructure". Other data which is subjected to data localisation rules are mapping services, online publishing, and telecommunications (World Bank, 2021).

[13] See the definition of sensitive data on page 14 of the Paper.

[14] The 2006 quote from mathematician Clive Humby is very misleading because it implies that all data has an equal value, whereas some data is very common/does not have much value, some is very rare – with a high value; nearly all data will reduce in value as it gets older. This is true for both personal and non-personal data.

[15] The Paper, pages 15 & 24. See also recommendation 10.3.2 which recognises the role of POPIA and PAIA. In some instances, the Paper confuses readers by introducing new privacy concepts (eg Sensitive Data – defined twice on page 14).

P O Box 1753, Jukskei Park, Gauteng 2153 RSA Tel: +27 11 704-0937 Email: info@ecomafrica.org
EFA is a Not For Profit Company, registration number 2020/110784/08 | FNB Account Number 6268.7019.664 / Branch 250655

theft of such data by either private or public entities. In this respect, EFSA is greatly concerned that one of the key advantages of data localisation is contrary to the fundamental rights of citizens and companies. This advantage, as pointed out above, is that localisation provides "greater efficiency in the data monitoring, owing to unfettered supervisory access of data". The seventh data privacy principle is accountability which is in contradiction to any unfettered access to data by government – or any other party.

EFSA recognises the privacy concerns raised by some 'Big Tech' companies' systems for processing data which they collect on their platforms. This point was raised by the Competition Commission in its paper on "Competition in the Digital Economy" and follow up "Online Intermediation Platforms Market Inquiry, Terms of Reference". This, as the Competition Commission recognised, is not just an issue in the RSA.[16] The debate in the EU and USA has led to a new privacy principle - the 'right to be forgotten' - which could be considered by RSA regulators.

However, it is difficult to understand how a data localisation policy would solve this privacy challenge. EFSA humbly suggests that this issue should be addressed by rules on **data sovereignty**. Data sovereignty is the concept that 'data are subject to the laws and governance structures within the nation it is collected'.[17] This differs from data localisation, which deals with rules on the locale of data storage - as we have seen above.

Data sovereignty also covers the protection of information (data) owned by businesses. EFSA notes that Australia has recently required Google to acknowledge and recompense news agencies from whom it takes news and other information. Thus data sovereignty also covers national laws relating to ownership of intellectual property. Business needs strong and unequivocable intellectual property rules to ensure economic growth and fair competition particularly for new sectors, such as the digital economy.

POPIA also requires clear ownership of personal data.[18]
This principle appears to be threatened by the statement that "*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 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*

[16] The Competition Commission. http://www.compcom.co.za/wp-content/uploads/2020/09/Competition-in-the-digital-economy_7-September-2020.pdf and http://www.compcom.co.za/wp-content/uploads/2021/02/OIPMI-Draft-ToR-19-02-2021.pdf
[17] A concept which is referred to in the Paper but not defined. The definition we use is from Wikipedia. EFSA fully supports data sovereignty which clarifies which national rules apply to data ownership and processing.
[18] The statement on page 26 of the Paper that data is "*sold globally for advertising purposes"* by technology companies, misleads by over-simplification. For example, personal data collected in the process of a sale by ecommerce companies in SA is essential for the e-merchant to service the customer. Selling such data is most unlikely to benefit the merchant.

P O Box 1753, Jukskei Park, Gauteng 2153 RSA Tel: +27 11 704-0937 Email: info@ecomafrica.org
EFA is a Not For Profit Company, registration number 2020/110784/08 | FNB Account Number 6268.7019.664 / Branch 250655

sector which, if shared with government, could enhance government's planning and service delivery capability, without infringing on the rights of citizens".[19]

EFSA believes that some of the recommendations in the Paper run contrary to the protections provided by POPIA and is disturbed to read that a single data regulator reporting to the DCDT Minister should be established.[20] Parliament specifically created the Information Regulator to "give effect to the constitutional right to privacy" (POPIA 2(a)) as an independent body which reports directly to it, and not to a Ministry, in order to ensure independence. EFSA questions how the draft National Policy squares with the rights of both citizens and organisations to own data and intellectual property.

Data Localisation, South Africa, and the African Free Trade Area (AfCFTA)

An issue completely over-looked by the Paper is the engagement of South Africa in the AfCFTA, which aims to encourage greater intra-Africa trade – and therefore industry – by creating a free trade area, reducing tariffs, dismantling non-tariff barriers, and simulating innovative solutions such as the digital economy and ecommerce.

As we have shown earlier in this submission, data localisation rules undermine trade and economic growth, create barriers to cross-border trade by, for example, preventing the effective use of e-payment systems, and lowers a country's digital trade index.

The AfCFTA on the other hand invites South African business and government to benefit from the economies of scale which the continent potentially offers. Data localisation will undermine the ability for South Africa to benefit from the opportunities afforded by the AfCFTA.

Currently there are four hyperscale data centres operating on the continent, all located in South Africa. Our country is the recognised leader in Cloud, however, if RSA introduces data localisation it will cause two probable scenarios – first, other countries, particularly small African nations without the server or cybersecurity capacity of South Africa may follow SA's lead. This would undermine the benefits of the AfCFTA and place many millions of African citizens at great risk of having their data compromised. Second, SA's existing data centres will lose their attractiveness for data storage from other countries, and those countries may also apply similar protectionist barriers against the RSA.

South Africa has a leadership role within the AfCFTA. It stands to be one of the major net beneficiaries of greater trade within Africa and a renaissance of manufacturing and service provision will provide RSA's citizens with new employment opportunities within the economy. The government is promoting constructive policies to attract investment in digital economy-related business.[21] All this will depend on whether the digital economy is allowed to grow or is contained by misguided data localisation regulation. If SA's economy is

[19] The Paper, Section 10.2, pages 20-21
[20] Ibid, Recommendation 10.6.2
[21] For example, the Paper, page 17, points out *"…measures to ensure that South Africa is an attractive host to the data centre industry on the African continent are necessary."*

P O Box 1753, Jukskei Park, Gauteng 2153 RSA Tel: +27 11 704-0937 Email: info@ecomafrica.org
EFA is a Not For Profit Company, registration number 2020/110784/08 | FNB Account Number 6268.7019.664 / Branch 250655

dampened, other African states will take and exploit SA's potential advantages provided by the AfCFTA.

EFSA believes strongly that government needs to consider very carefully any policies which will reduce SA's competitive advantages, and leadership role within the AfCFTA.

Conclusions

The Draft National Policy on Data and Cloud contains a number of positive recommendations as EFSA outlines at the start of this submission.

The main thrust of the Paper, however, calls for a National Open Data Strategy, the construction of a High-Performance Computing and Data Processing Centre (HPCDPC), a State Digital Infrastructure Company (SDIC). These initiatives will be supported by the imposition of an overarching data localisation policy.

An overall objective is to promote regulation that encourages the sharing of data between private and public data processors. The concern that EFSA expresses is that this sharing of data through the HPCDPC may not be voluntary for business data owners, and that government access to business data will compromise business data ownership, data security, the privacy of data subjects and undermine intellectual property ownership. Control of access to data (whether localized or not), is a principle governed by data sovereignty. This issue may cause digital trust between the government and the governed to be undermined.

Our concerns are based on the lack of clarity in the Paper – as for example in Recommendation 10.4.4, which states:
"*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. ….*
- *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….*
- *The Department of Trade, Industry and Competition though the Companies and Intellectual Property Commission (CIPC) and the National Intellectual Property Commission (NIPMO) shall develop a policy framework on data generated from intellectual activities including sharing and use of such data."* [22]

The Paper points out several times that government data is placed in many silos, which prevents it from being used effectively to serve the citizen or business. EFSA humbly suggests that, rather than trying to tap into privately owned data, government should first

[22] Ibid, pages 27-28

P O Box 1753, Jukskei Park, Gauteng 2153 RSA Tel: +27 11 704-0937 Email: info@ecomafrica.org

find assistance to amalgamate its data centres (an objective of the HPDCPC) and data-mine these to assist it in providing improved services to citizens. [23]

On the evidence, EFSA suggests that data localisation will not benefit the South African economy, will not encourage businesses to develop; will discourage investment; will decrease cybersecurity; will reduce the protection of intellectual property, and the right to privacy. The policy will run counter to the benefits offered to the RSA by the AfCFTA. The Paper's argument that private data will assist government if access is made available via a national cloud storage service supported by localisation rules fails to persuade – what protection will be afforded to business or the citizen, what data would be involved, from which private owners and why is public data not sufficient for the government's needs?

EFSA therefore respectfully proposes that the aspects of the Paper relating to data localisation and any access to privately owned data be dropped.

Finally, as suggested above, EFA believes that the AfCFTA should in the future consider an African Cloud storage system once the economies of scale provide the required volume and the expertise of specialists to develop an African Cloud. Sharing such a service between the AU Member States would avoid undue national interference in an African Cloud.

12 May 2021

[23] Presently government held data is extensive thanks to the numerous interfaces it has with private citizens – data is collected by CIPC, RICA, FICA, and by Home Affairs. It is provided by pharmacies and hospitals for pharmaceutical use; by SARS on tax; from SAPS; the TV and vehicle licensing bodies; motorway tolls, etc, etc.

P O Box 1753, Jukskei Park, Gauteng 2153 RSA Tel: +27 11 704-0937 Email: info@ecomafrica.org
EFA is a Not For Profit Company, registration number 2020/110784/08 | FNB Account Number 6268.7019.664 / Branch 250655