



**Comments to the South African Reserve Bank on  
Consultation Paper on Cloud Computing and Offshoring of Data**

**May 2025**

The Global Data Alliance (“GDA”) welcomes the opportunity to share its views on the *Consultation Paper on Cloud Computing and Offshoring of Data* published by the South Africa Reserve Bank (SARB).<sup>1</sup>

**I. Executive Summary**

GDA member companies are active in South Africa in various types of financial and insurance services, as well as various cloud computing and other software and ICT services. The GDA supports many of the stated objectives outlined in the consultation paper. However, the GDA does not support the paper’s proposals for financial data localization requirements. These are not effective or necessary in implementing paper’s stated objectives. If anything, imposing data localization mandates will undermine those objectives.

While GDA members do often employ South Africa-based cloud computing infrastructure, the GDA is of the unequivocal view that it would be a mistake for SARB to mandate strict compliance with requirements to localize data or infrastructure in South Africa. Instead of imposing such mandates, we urge SARB to focus on safeguarding regulatory priorities through functional requirements that allow data to be transferred and stored across transnational digital networks. In short, SARB should allow data to be transferred and stored in the cloud, provided that – in SARB’s phrasing – “payment institutions and operators remain in compliance with ... relevant [functional] requirements.” Para. 9.2.

**II. About the GDA**

The GDA is a cross-industry coalition of companies committed to high standards of data responsibility, privacy, and security.<sup>2</sup> Our members rely on the ability to transfer data across borders to innovate, create jobs, and deliver services across various sectors, including agriculture, automotive, biopharmaceuticals, finance, healthcare, insurance, logistics, payment processing, and telecommunications. Alliance member companies include domestic oriented businesses in South Africa that collectively invest billions of dollars in the South African economy, employing tens of thousands of South African citizens, and supporting numerous activities that advance inclusive growth, innovation, and economic development in South Africa.

Among other things, Alliance members help provide to South Africa financial services, enterprise software technologies, and health, scientific and educational resources. Alliance members also help make local enterprises, including micro-, small-, and medium-sized enterprises (MSMEs), more competitive globally. Alliance members also help deliver telecommunications and cloud-based technology solutions across South Africa, supporting broadband connectivity within South Africa and across neighboring markets.

### III. Recommendations

The GDA respectfully urges SARB:

**Not to advance proposed localization requirements in Section 9.3.** This includes mandates for:

- Localization of clearing and settlement services, data, and other systems (para. 9.3.1.a-b);
- Localization of cloud computing services and infrastructure (para. 9.3.1.c)

**Not to advance the “cloud location” requirements in Section 9.4.** This includes mandates for:

- Localization of cloud computing infrastructure for payment systems, clearing and settlement activities (para. 9.4.3.a-c).

**Not to advance the proposed requirement that regulated entities** secure SARB’s pre-approval prior to other cloud utilization and international data storage activities.

To protect South Africa’s integration within the broader global financial system, and to protect other benefits transnational cloud computing offers, it is essential that SARB not advance these localization mandates. We elaborate below.

### IV. GDA Supports Certain Aspects of the Consultation Paper

The GDA agrees with many perspectives outlined in the Consultation Paper. For example, we agree that the use of transnational cloud computing resources can benefit South African citizens by offering:

- (1) **Greater functionality** for the benefit of South African citizens (§ 5.3.1);
- (2) **Improved capacity** for ensuring data integrity and security (§ 5.3.2);
- (3) **Global access** for South African customers from their devices anywhere in the world (§ 5.3.3);
- (4) **More efficiency** in multi-media support for those customers (§ 5.3.4); and
- (5) **Data analytics**-driven services improvements powered with global or regional data sources; (§ 5.3.5).

We also agree with SARB that cloud computing resources can advance South African interests in:

- (6) **Lower costs, scalability, and efficiency** in financial services (§ 6.1);
- (7) **Reduced barriers to entry and greater competition** via a leveling of the playing field between large payment institutions and small- to medium-sized payment institutions, which are often local enterprises (§ 6.2);
- (8) **Greater speed, transparency, and availability** of cross-border payments for the benefit of all South African citizens, consistent with the key objectives in the G-20 cross-border payments programme (§ 6.3);
- (9) **Increased data security and cyber-resilience**, given the greater ability to protect the confidentiality and integrity data, not to mention system-wide security, as highlighted in the consultation feedback received by Financial Stability Board in this regard (§ 6.4);
- (10) **Real-time, 24/7 response capacity** and redundancy as a backstop against operational failures or events impacting onshore teams (§ 6.5);
- (11) **Access to global skills and talent** (§ 6.6); and
- (12) **Increased agility** to respond to changes in demand and market conditions (§ 6.7).

## V. GDA Welcomes the Opportunity to Inform Other Aspects of the Consultation Paper

The GDA take a different view of the “risks associated with cloud computing and data offshoring” from the perspective articulated in Section 7 of the consultation paper. We address the main points below.

- (1) **Data Transfers & Cloud Computing Do Not Increase Operational Risk:** The consultation paper suggests that use of international cloud services may increase operational risk. (§ 7.1). We disagree. In fact, as SARB itself recognizes in Section 6.4, use of centralized cloud services reduces various data security and cyber-related risks. Instead of requiring data localization, SARB should focus on functional operational risk mitigation practices that are applied regardless of where data may be situated.
- (2) **Data Transfers & Cloud Computing Do Not Increase Reputational Risk:** The consultation paper states that “adopting cloud computing... without a ... framework that supports safety and efficiency could result in reputational risk.” (§ 7.2). We observe that SARB has developed a framework focused on these functional outcomes, obviating the stated rationale for localization mandates. Furthermore, as SARB acknowledges in Sections 5.3, 6.1, 6.3, and 6.4 use of cloud computing will improve efficiency, functionality, safety, and security for South African citizens. Conversely, prohibitions on the use of cloud computing will undermine those objectives. It is precisely the imposition of localization mandates that will increase reputational risk for SARB.
- (3) **Data Transfers & Cloud Computing Do Not Reduce Transparency:** The consultation paper implies that cloud service arrangements lack transparency. (§ 7.3). However, in Section 5.3, SARB recognizes that use of cloud services can increase transparency. Furthermore, operators and other private parties can negotiate for greater contractual transparency in a competitive cloud marketplace. Reducing competition and choice by mandating data localization will make this more – not less – difficult.
- (4) **Data Transfers & Cloud Computing Do Not Engender Concentration Risk or Systemic Risk:** The consultation paper states that cloud computing in South Africa is prone to concentration or systemic risk (§§ 7.4-7.6). However, surveys of South Africa’s cloud marketplace indicate that the market is served by a diversity of service providers based in various regions and countries.<sup>3</sup> Furthermore, mandating data localization or use of local cloud services will have the opposite of the intended effect. Localization mandates only serve to decrease the number of available cloud service providers, thus exacerbating the risk identified by SARB. Simply put, permitting access to cloud services from numerous other economies reduces the “concentration risk” or “systemic risk” described. Conversely, imposing localization mandates increase those risks by limiting access to cloud services in or from a single economy.
- (5) **Data Transfers & Cloud Computing Do Not Worsen Security Risks:** The consultation paper raises concerns regarding cybersecurity risks in connection with data transfers and cloud computing. (§ 7.8). However, SARB recognizes in Section 6.4 that cross-border data transfers in the cloud actually reduce cybersecurity risk.
- (6) **Data Transfers & Cloud Computing Do Not Exacerbate Geopolitical Risk:** The consultation paper raises legal and political risk concerns regarding cloud storage in a single foreign jurisdiction. First, the GDA observes that, as reflected in Figures 4-5 of the consultation paper, cloud service infrastructure is widely distributed in dozens of economies across all six continents. The perception that cloud infrastructure is limited or restricted to just one or two economies is misplaced. Furthermore, it hardly seems reasonable to mandate – as a response to that misperception – the localization of cloud infrastructure in a single economy.

## VI. Economic Impacts

The localization mandates proposed in the consultation paper would increase economic risks for South Africa, as outlined below.

- **Impact on South Africa's Economy:** The World Bank's 2020 *World Development Report* found that, "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies... Countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5 percent."<sup>4</sup> Conversely, data localization imposes heavy costs on economies that adopt such measures:
  - Forced data localization is estimated to [reduce GDP by 0.7%–1.7%](#). Such restrictions would reduce South Africa's economic growth, slow productivity, and increase prices for South African governmental authorities, businesses, and citizens.<sup>5</sup>
  - Forced data localization is associated with [investment decreases of up to 4%](#). Foreign investment supports millions of jobs in South Africa. SARB's recommended localization mandates could reduce South Africa's relative attractiveness as a destination for foreign investment.
  - Forced data localization combined with data flow restrictions are estimated to [reduce exports by 8.5%](#). As one of the largest exporters in Africa, South Africa benefits greatly from its integration within the global economy. The potential impacts on South African exports and jobs due to data localization mandates like those proposed in the consultation paper should not be lightly dismissed.
- **Impact on South African Services:** The World Bank 2021 *World Development Report* has noted that measures that "restrict cross-border data flows ... [may] materially affect a country's competitive edge in the burgeoning trade of data-enabled services."<sup>6</sup> A 2020 World Economic Forum study found that, "approximately half of cross-border [services] trade is enabled by digital connectivity[, which] ... has allowed developing countries and micro, small and medium-sized enterprises (MSMEs) to export through greater visibility, easier market access and less costly distribution."<sup>7</sup> In 2024, South Africa exported over \$2 billion in services to the United States, in travel, professional and management services, and the transportation sector – all areas that are heavily dependent on cross-border access to technology and data transfers.<sup>8</sup> Imposing the localization requirements proposed in the consultation paper will undermine those exports.
- **Impact on South Africa's Position as Regional Center of Cloud Computing Services:** South Africa is currently a regional leader in offering cloud computing services to neighboring economies. South Africa's policy positions also have broad regional influence. South Africa risks losing its position as a regional provider of cloud services, if its neighboring economies emulate the cross-border data restrictions found in the consultation paper.

## VII. Policy Impacts

The data localization requirements proposed in the consultation paper may also undermine public policy goals relating to the health, privacy, and security of persons in South Africa. We address these topics below.<sup>9</sup>

- **Impact on ICT Policies:** From artificial intelligence to 5G to the cloud, governmental ICT policies can help coordinate public-private dialogue, support investment, and maximize the benefits of ICT technologies across the economy. Cross-border data restrictions often undermine these policies. For example, the benefits of cloud computing policies are most likely to arise in a cross-border context that allows for elastic and scalable delivery of computing resources, rapid load balancing, and ready access to best-in-class technology from all over the world. Using data localization mandates and transfer restrictions to ban cross-border access to cloud computing infrastructure and technology would deprive local enterprises (including MSMEs) and users of:
  - Cross-border access to IT resources hosted abroad;
  - Cross-border collaboration and communication with foreign business partners;
  - Foreign transactions and business opportunities; and
  - Improved resiliency resulting from data storage across multiple geographical locations.<sup>10</sup>
- **Impact on Cybersecurity:** Some argue that cross-border data restrictions are necessary to ensure cybersecurity. However, *how* data is protected is more important to security than *where* it is stored, and transfer restrictions often result in *weaker*, not *stronger*, cybersecurity. Cross-border data transfers help improve cybersecurity because these transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Stronger cybersecurity is enabled by cross-border data analytics and an assertive cyber-defense posture coordinated across IT networks and national boundaries.<sup>11</sup> When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities.<sup>12</sup> The GDA encourages SARB to focus on operational risk management requirements or specific guidance concerning how cloud services relates to the NPSD's existing Directive on Cybersecurity and Cyber Resilience within the National Payment System.
- **Impact on Privacy:** Some argue that cross-border data restrictions are necessary for privacy reasons – i.e., to ensure that companies process and use data consistent with a country's data protection laws. In fact, organizations that transfer data globally typically implement procedures to ensure that the data is protected even when transferred outside of the country. To that end, organizations often rely on various approved data transfer mechanisms.
- **Impact on Regulatory Compliance:** Some claim that cross-border data restrictions ensure governmental access to data for regulatory or investigatory purposes. The location of the data, however, is not the determining factor. On the contrary, "data localization requirements can increase ... operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information."<sup>13</sup> Accordingly, regulatory authorities in many countries actually encourage the responsible transfer and storage of data across digital networks. Likewise, cross-border access to financial data is critical to other public policy priorities, including financial fraud monitoring and prevention; anti-money laundering; anti-corruption; and other financial regulatory compliance objectives.
- **Impact on Innovation:** Some claim that cross-border data restrictions promote innovation. On the contrary, data localization mandates, data transfer restrictions and approval requirements undermine beneficial innovation processes—from accessing global scientific and technical research databases, to engaging in cross-border research and development

(R&D), to securing intellectual property rights for new inventions, and regulatory product approvals for new products and services.<sup>14</sup> Imposition of such approval requirements results in time delays and high bureaucratic burden, which serves to delay cloud migrations, change management, and innovation and service improvements that would otherwise benefit South African customers and citizens.

## VIII. Conclusion

In conclusion, we respectfully recommend that SARB not adopt any of the data localization proposals in the consultation paper. We appreciate the opportunity to share these views and hope that they will be helpful as SARB considers its next steps. Please do not hesitate to contact us with any questions regarding this submission.

<sup>1</sup> [https://www.reservebank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight-and-supervision/document-for-comments/doc-for-comments-2025/Cloud%20computing%20and%20offshoring%20of%20data%20consultation%20paper\\_March%202025.pdf](https://www.reservebank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight-and-supervision/document-for-comments/doc-for-comments-2025/Cloud%20computing%20and%20offshoring%20of%20data%20consultation%20paper_March%202025.pdf)

<sup>2</sup> For more information, please see [www.globaldataalliance.org](http://www.globaldataalliance.org)

<sup>3</sup> *Cloud Infrastructure South Africa* (2024), at: <https://www.datacentermap.com/cloud/g/south-africa/>

<sup>4</sup> World Bank, *World Development Report* (2020), at: <https://www.worldbank.org/en/publication/wdr2020>

<sup>5</sup> See APEC, *Economic Impact of Adopting Digital Trade Rules* (2023), <https://www.apec.org/publications/2023/04/economic-impact-of-adopting-digital-trade-rules-evidence-from-apec-member-economies> See also WTO/OECD Report (complete cite) (“When [data localization requirements] are combined with flow prohibitions, even if only for a limited set of sectors (financial, telecommunications, and ICT services), impacts can rise quickly. If all economies adopt these, GDP would fall by 0.5% and exports by nearly 1%.”)

<sup>6</sup> World Bank, *World Development Report – Data For Better Lives* (2021), at: <https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000.pdf>

<sup>7</sup> World Economic Forum, *Paths Towards Free and Trusted Data Flows* (2020).

<sup>8</sup> See e.g., Office of the US Trade Representative, *US-South Africa Trade Relationship* (2019), at: <https://ustr.gov/countries-regions/africa/southern-africa/south-africa>

<sup>9</sup> For additional information, see [https://www.globaldataalliance.org/downloads/02112020\[crossborderdata.pdf](https://www.globaldataalliance.org/downloads/02112020[crossborderdata.pdf)

<sup>10</sup> See generally, BSA, *Moving to the Cloud – A Primer on Cloud Computing* (2018), at [https://www.bsa.org/files/reports/2018BSA\\_MovingtotheCloud.pdf](https://www.bsa.org/files/reports/2018BSA_MovingtotheCloud.pdf).

<sup>11</sup> See *id.* Cloud services delivered across-borders provide security advantages over alternative IT delivery approaches (on-premises or local cloud services):

- Physical Security: Certified personnel can carefully monitor servers 24/7 to prevent physical breaches, and can apply consistent protocols over a small number of locations.
- Data Security: CSPs can ensure data integrity through use of state-of-the-art encryption protocols for data at-rest and in-transit. CSPs can establish redundant backups of data in geographically dispersed data centers, mitigating risk of loss in the event of power outages or natural or manmade disasters.
- Advanced Threat Detection: CSPs leverage state-of-the-art enhanced security intelligence. They use regular penetration testing to simulate real-world attacks and evaluate security protocols against emerging threats.
- Automated Patch Deployment: Automated and centralized patch deployment and realtime updates to network security protocols work to protect systems from newly identified vulnerabilities.
- Incident Management and Response: CSPs maintain global teams of incident response professionals to respond and mitigate the effects of attacks and malicious activity.
- Certification: CSPs are typically certified to international security standards, and go through regular audits to maintain their certifications.

<sup>12</sup> See *id.*, p. 1.

<sup>13</sup> See e.g., United States-Singapore Joint Statement on Financial Services Data Connectivity, at: <https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity>;

<sup>14</sup> See Global Data Alliance, *Cross-Border Data Transfers and Innovation* (2021), at <https://globaldataalliance.org/downloads/04012021cbdtinnovation.pdf>