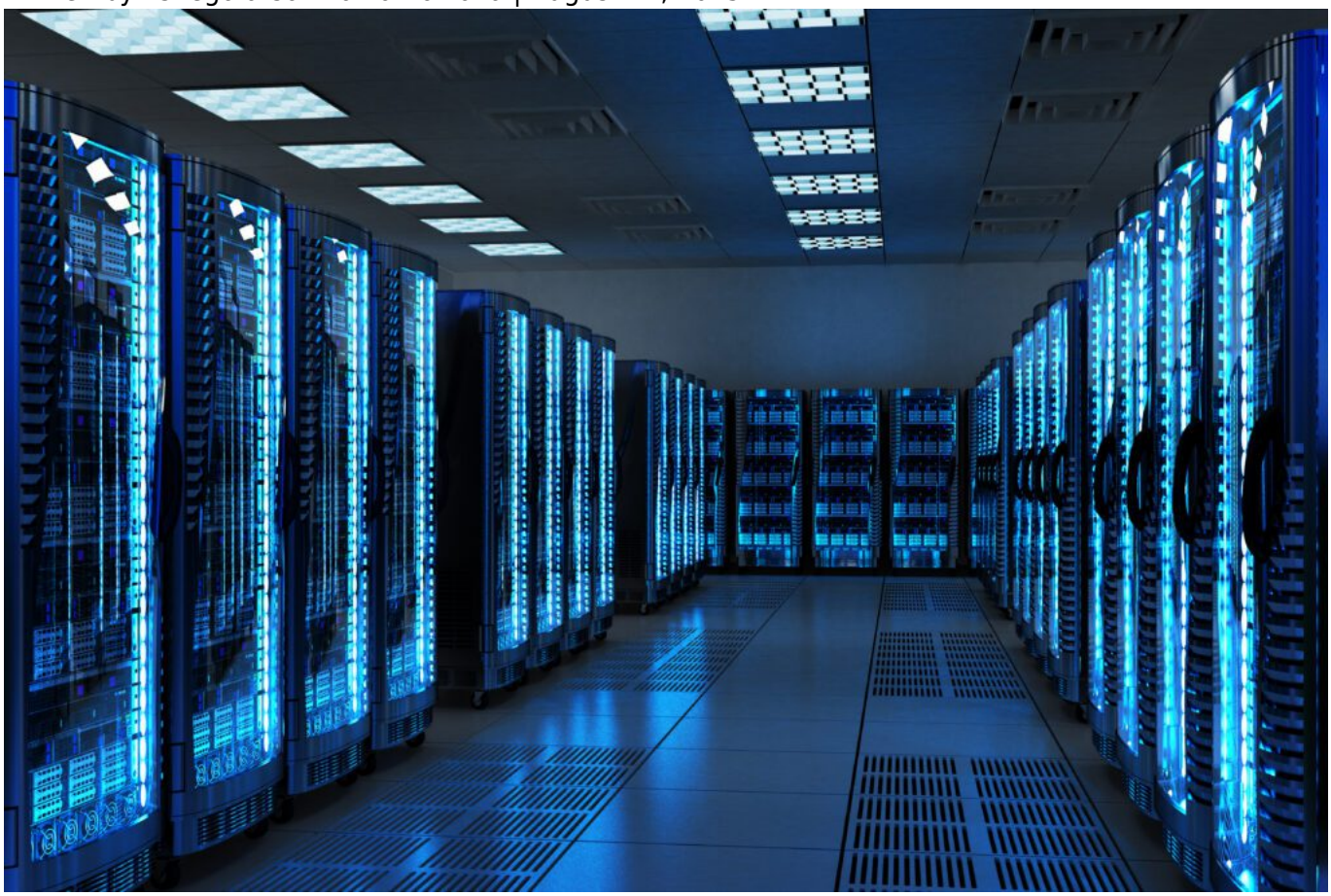
DATA IN THE CLOUD, BUT GROUNDED BY GOVERNANCE: FSCA AND PA SET TO REGULATE CLOUD COMPUTING AND DATA OFFSHORING

Category: IT Law,Technology Law
written by Tshegofatso Phahlamohlaka | August 11, 2025



In a move that signals a step forward in data governance for South Africa's financial sector, the Financial Sector Conduct Authority ("**FSCA**") and the Prudential Authority ("**PA**") (together referred to as the "**Authorities**") have issued a Joint Communication on the use of cloud computing and data offshoring by financial institutions. The Authorities plan to introduce a Joint Standard targeted at financial institutions, which will outline regulatory requirements for the use of cloud computing and data offshoring.

What is the Big Deal about the Cloud? And What Should Financial Institutions be thinking about?

Imagine instead of buying your own massive computer servers and maintaining them in-house you rent computing storage and software from a provider like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud. These providers host the technology and is accessed over the internet. On the other hand, data offshoring is when your data (client information or transaction records) is stored or processed outside South Africa's borders. While the use of these services offers efficiency and improved operations, it also introduces important legal, regulatory and cybersecurity risks and concerns. The Authorities aim to address some of these issues through regulation and guidance.

Why This Joint Communication Matters

The Authorities issued the joint communication to:

1. inform financial institutions of risk mitigation measures when using cloud services or offshoring data;
2. highlight the important role of boards of directors and senior management in overseeing these decisions; and
3. signal the forthcoming publication of a Joint Standard that will introduce regulatory requirements for the use of cloud computing and data offshoring.

What Should Financial Institutions Do Right Now?

While the Joint Standard is still in development, the Authorities have outlined interim expectations which financial institutions need to adopt, including:

1. Adopting a risk-based approach when using cloud services or offshoring data, that their cloud decisions must reflect their institution's size, complexity, and risk appetite.
2. Establishing and implementing appropriate governance structures, processes, and procedures to oversee the use of cloud computing. This includes:
    1. a board-approved cloud/data strategy;
    1. a clear data governance framework; and
    1. implementing reasonable measures to ensure the confidentiality, integrity and availability of their data, information technology applications or systems.

3. Conducting due diligence before entering any cloud or offshoring arrangement, this includes, reviewing contractual obligations, and evaluating cybersecurity and data protection measures.

Important Considerations

Some of the key questions that financial institutions need to ask are:

1. Does the organisation have a clear policy on what data can live in the cloud and where?
2. Is the organisation prepared for the risks of offshoring sensitive data?
3. Are the cloud and offshoring risks documented?
4. Who is responsible when there is a breach on a third-party cloud provider?
5. How is the organisation ensuring data surety, confidentiality, privacy, and availability?

What is Next?

The Authorities are in the process of developing a Joint Standard, which will be released for public consultation. In parallel, the Authorities will be strengthening their supervisory capabilities throughout 2025 and 2026, with a focus on incorporating cloud computing and offshoring risks into routine regulatory assessments. The Authorities will continue to monitor how financial institutions have approached the integration of cloud computing and/or data offshoring risks into their

governance, risk management and reporting processes.

Contact us for good, clear, precise advise!