Cloud sovereignty for the AI age

Gert Haasbroek, Senior Cloud Architect at Datacentrix

Cloud sovereignty has become one of the most discussed topics within the technology industry, yet it is also one of the most misunderstood. Much of this confusion stems from the assumption that sovereignty is guaranteed simply because data is hosted locally.

In reality, true sovereignty extends far beyond where information is stored, and South African organisations need to move past marketing claims and ask deeper questions about control, accountability and governance.

The first principle of sovereignty is that it should be defined in the contract. Every provider promises sovereignty, but companies need to understand exactly what sits behind those claims. Questions such as who owns the underlying infrastructure, who manages it, where the management plane resides, and whether third-party software dependencies introduce external jurisdictional exposure are becoming increasingly important.

For local cloud providers, sovereignty cannot be a bolt-on service. At Datacentrix, for instance, infrastructure is owned and operated locally, while management and operational teams are based within South Africa. This creates greater ability to provide genuine local accountability, transparency and contractual flexibility.

This is particularly important for highly regulated sectors such as financial services, government and healthcare, where sovereignty is increasingly a compliance requirement rather than a competitive differentiator.

Changing the sovereignty equation

The conversation becomes significantly more complex when AI enters the picture. Historically, organisations focused on where data was stored, but AI shifts the discussion towards where data is processed, how it is transformed and who may ultimately have access to it. Even locally developed AI solutions frequently interact with global AI engines, creating new sovereignty challenges that previously might not have been considered.

> “At Datacentrix, for instance, infrastructure is owned and operated locally, while management and operational teams are based within South Africa. This creates greater ability to provide genuine local accountability, transparency and contractual flexibility.

Every interaction with an AI platform potentially contributes data to a broader ecosystem. When organisations develop AI solutions locally, or when individuals use global AI platforms, information does not simply remain in one location. It is processed, transformed and, in some cases, used to improve the models themselves. Information that appears harmless

in isolation can reveal more than users realise when aggregated and analysed. As a result, sovereignty can no longer be viewed solely through the lens of physical data location.

Even something as simple as a parent asking an AI tool to generate a Grade 4 English exam can reveal information. The request is processed globally, and these small pieces of information can accumulate, often without users realising what they are sharing. Anything entered into these systems is generally logged and retained in some form and once that information enters the platform, it is no longer fully controlled by the user.

The challenge is enormous because, at present, convenience is winning over governance and there is no clear picture on how this will be controlled. Potentially, future governance will need to come from a much higher level than individual cloud providers. Governments and regulators will likely have to introduce frameworks to prevent sensitive information from crossing borders inappropriately.

What is apparent, however, is that AI is exposing data to a much more global environment than organisations have traditionally dealt with.

PoPIA's effect on cloud procurement

This changing landscape is also influencing how companies purchase cloud services. The Protection of Personal Information Act (PoPIA) has fundamentally altered procurement discussions. When evaluating local cloud providers, compliance teams now sit alongside technical, commercial and executive stakeholders.

Importantly, PoPIA places accountability on the organisation, not the cloud provider. While providers play a critical role in securing infrastructure and protecting workloads, businesses remain responsible for ensuring that personal information is processed lawfully and in accordance with regulatory requirements. Selecting a provider based solely on price or convenience – without properly interrogating compliance commitments – creates unnecessary risk.

The Information Regulator has also made it clear that enforcement activity is increasing, making documented answers to key questions around sovereignty, security and governance more important than ever. Simply stating that a cloud provider was trusted will not be an adequate defence if a breach were to occur.

Gert Haasbroek Senior Cloud Architect at Datacentrix

Sovereignty requires ongoing governance

Good sovereign cloud governance ultimately requires an ongoing commitment rather than being considered as a one-time tick box exercise. It begins with understanding which data and workloads require stricter protection, supported by a clear classification framework, robust contracts and strong technical controls. Organisations should also maintain independent audit rights and regularly validate that providers continue to deliver on their contractual commitments.

At the same time, cloud providers must ensure transparency around infrastructure management, security controls and incident response processes. Sovereignty works best when it is treated as a shared responsibility, with providers securing the infrastructure and customers actively governing how their information is managed and protected.

As AI becomes more deeply embedded in business operations, sovereignty will be defined less by where data resides and more by who controls it, how it is used and who is accountable for it. Organisations that ask the right questions today, and can demonstrate genuine control over their data environments, will be far better positioned to navigate the regulatory, operational and governance challenges that lie ahead.

For more information contact
Elzette du Preez at edupreez@datacentrix.co.za