

ON TRACK AI INSIGHTS

Sovereign AI in South Africa

What it actually means here

Deon Thomas
CEO, eBlocks Software

eblocks.co.za
7 min read



What follows.

- I The part nobody presents**
Why the exposure is not where your data sits

- II What sovereign AI means**
A definition that fits in one sentence

- III What South Africa already requires**
POPIA, the cloud directives, and what they bind

- IV Three layers, not one**
Where most sovereignty reviews stop

- V The question none of it answers**
And why it gets asked in the same meeting



The part nobody presents.

A foreign court order does not land in your inbox.

The letter does not arrive at your desk.

A foreign court order compelling your cloud provider does not land in your inbox. It lands on the provider. In many cases you are not told it arrived, and you are not told what left.

That is the part of sovereignty nobody presents to a board. The exposure is not that your data is somewhere foreign. It is that the decision about your data can be made by someone else, under a law you have never read, in a jurisdiction you have never operated in — and you may find out afterwards.

Most South African enterprises have been discussing sovereign AI for eighteen months. Very few can say which of those scenarios they have actually closed.

The framing came from elsewhere. In Europe it is about the AI Act. In the United States it is about chips and national capability. Neither helps a bank in Sandton decide where to run a model.

The local question is narrower. Can an enterprise under South African law account for what its AI does, where the data sits, and whose courts can reach it?



What sovereign AI means.

A definition that fits in one sentence.

AI you keep legal control of.

Your data, your model, and the systems running them stay under your own country's law, and out of reach of anyone else's.

That definition does two things. It separates sovereignty from patriotism, which is where most commentary goes wrong. And it makes the real point: this is a question about law, not geography.

**Residency is where.
Sovereignty is whose.**

The distinction the whole topic turns on.

The order reaches the provider. Not you.

FOREIGN COURT

issues the order



YOUR PROVIDER

receives it, and must comply



YOU

are not necessarily told

The decision is made somewhere you are not.



What South Africa already requires.

There is no AI Act here. There is a stack of law that already binds you.

The rules predate your AI.



POPIA has been fully enforceable since July 2021. It restricts cross-border transfers unless the recipient is under protections substantially similar to its own. Amended regulations took effect in April 2025.

Penalties reach R10 million, and in severe cases, imprisonment — for responsible individuals, not the company. For banks, the Prudential Authority's directives have governed cloud and offshoring since 2018.

IV

Three layers, not one.

Where most sovereignty reviews stop.

Three things, not one.

Most sovereignty reviews check where the data sits and stop there. That is one layer of three.

Your data. Where it lives, and who can demand it. This is the layer everyone checks, and the only one most vendor questionnaires ask about.

Your model. What it was trained on, and who holds the weights. A model you call over an API is a model somebody else controls. If they change it, retire it, or are compelled to disclose what passed through it, none of that is your decision.

Your operations. Who runs the system, under whose law, and who holds the keys. A local data centre operated by a foreign entity is a local building under foreign control.

A review that clears the first layer and ignores the other two has not established sovereignty. It has established residency and filed it under a different name.

**Most reviews check
only the first.**

Four moves, in order of how much they change.

01 Know which layer you have solved

Write down what you have verified for the model and operations layers, not just the data layer. The gap is usually the finding.

02 Ask the jurisdiction question directly

Not where the data is stored. Which entity is the contracting party, and which law governs it. The answer is often a different company to the one on the invoice.

03 Separate what needs sovereignty from what does not

Not every workload does. Treating everything as sovereign is expensive and slows down the things that could have moved fast.

04 Decide it at design time

Sovereignty is cheap to build in and expensive to retrofit. It is an architecture decision, not a procurement one.

V

The question none of it answers.

You can solve all three layers and still not be able to answer it.

And you will still be asked what the AI did.

Local data. Local model. Local operations. Contracts under South African law. Every box ticked, signed off, presented to the board.

Sovereignty tells a regulator where your systems run and whose law governs them. It says nothing about whether the thing you shipped is the thing your business asked for.

Directive 3 does not only require you to know where your data is. It requires that your arrangements do not inhibit a regulator's ability to do its job. "The AI decided" does not meet that standard in any jurisdiction.

01 What did the business request?

02 Who approved it?

03 Where is the test that proves it works?

04 What did the AI cost against what it delivered?

Two questions. One meeting.

01

Where does it run, and under whose law?

02

What did it do, and who said so?

Most organisations have prepared for one of them.

Bring the document it was built from.

Twenty minutes, in your own board. We will walk it through the loop and show you exactly where the evidence breaks.

eblocks.co.za/ontrack-ai

Book a demo →

Deon Thomas · CEO, eBlocks Software
solutions@eblocks.co.za

What this is built on.

Protection of Personal Information Act 4 of 2013

Fully enforceable from 1 July 2021. Amended regulations effective April 2025.

National Data and Cloud Policy

Published 31 May 2024, Department of Communications and Digital Technologies.

Directive 3 of 2018 and Guidance Note 5 of 2018

Prudential Authority, SARB. Effective 1 October 2018.

Joint Standard on Cybersecurity and Cyber Resilience

Prudential Authority and FSCA. In force from June 2025.

Clarifying Lawful Overseas Use of Data Act

United States, 2018.

National AI Policy Framework

Department of Communications and Digital Technologies, October 2024.

General commentary, not legal advice.