Keeping up with **compliance**

Your 2025 guide to staying protected

vodacom business

Cloud compliance is evolving **fast,** and the stakes are higher than ever. South Africa's data laws have teeth, and businesses that don't adapt risk more than just reputational damage — **they face operational disruption, legal exposure, and customer fallout.**

That's why we've put this **guide** together for you. We know the rules are shifting, and it's tough to keep up. So, we've **done the digging, tracked the amendments, and compiled what really matters.**

vodacom business

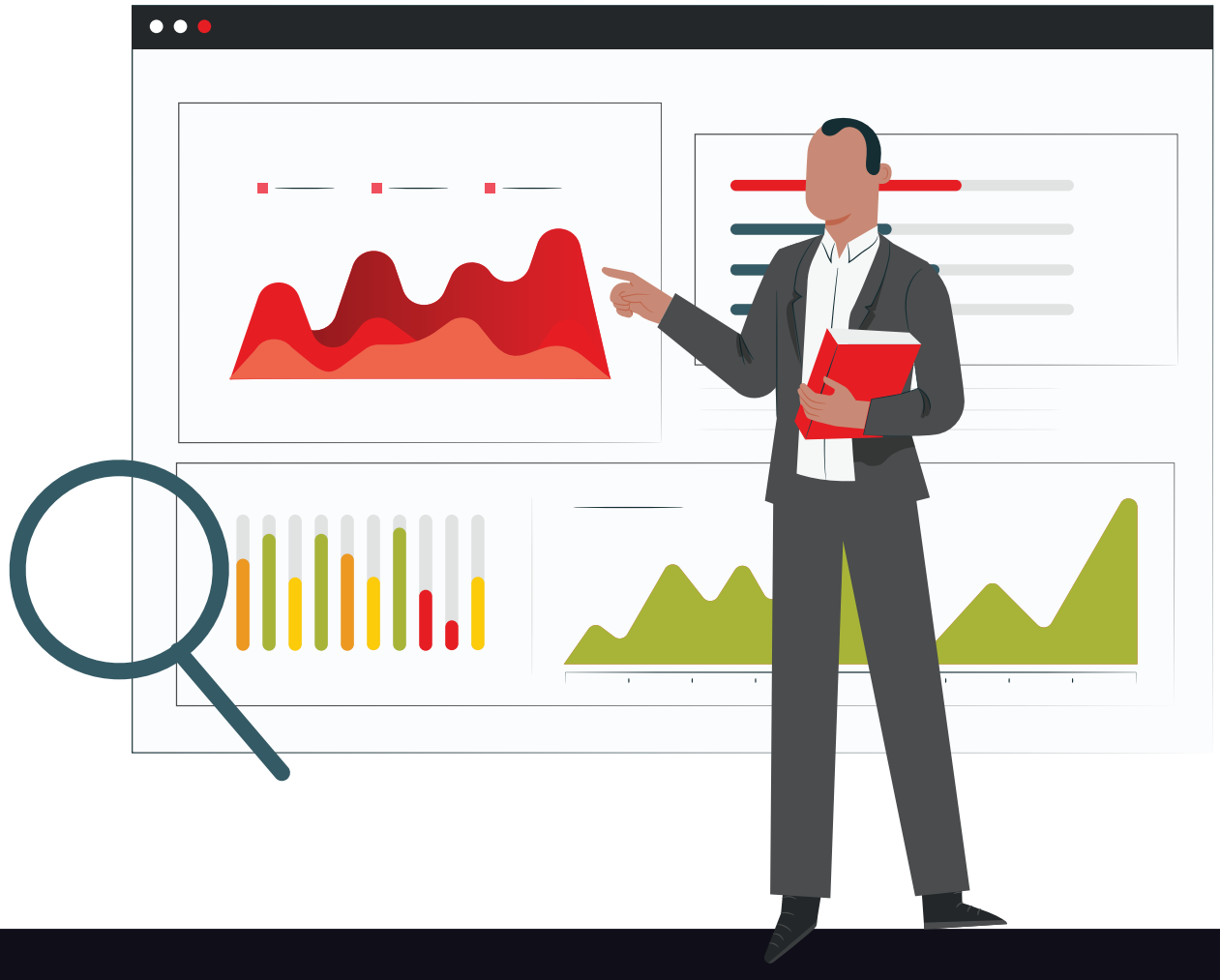
Why cloud compliance matters **more than ever**

Regulatory enforcement has stepped up. Data breaches are more frequent. And public trust in digital services hinges on privacy. IT and compliance teams now face a dual challenge:

Staying competitive with cloud innovation

Meeting the strict requirements of data protection laws

With enforcement powers expanded and new administrative fines introduced, **non-compliance is now a greater risk than ever.**



vodacom business

Key POPIA sections that matter for cloud adoption

Section 19 – Security safeguards

This section requires that personal data be protected through appropriate security measures. For cloud adoption, this means your provider must implement strong technical and organisational controls — like encryption, access management, and breach detection — to reduce your risk exposure. Weak safeguards on their side put your compliance at risk.

Section 72 – Cross-border transfers

Cloud providers often store or process data in global regions. This section ensures that if data leaves South Africa, it must go to a jurisdiction with equivalent protection, and only with the data subject's consent. Choosing a cloud provider without a clear cross-border policy could land your business in legal hot water.

Section 8 – Accountability

POPIA places the responsibility for lawful data handling on the responsible party — that's you. But when you use a cloud provider, you need full visibility into how they process your data. This section makes transparency and traceability critical — you can't just 'trust' your provider; you need proof.

Section 5 – Data subject rights

POPIA gives people rights over their own information, including access, correction, and deletion. Your cloud provider must enable your business to honour these requests quickly and easily. If their systems are opaque or uncooperative, your compliance breaks down.

Section 21 – Due diligence

Before you sign with a cloud provider, you're legally required to ensure they meet POPIA's standards. This means documented vetting of their policies, certifications, and practices — not just a tick-box SLA. Section 21 makes it clear: ignorance is not a defence.

vodacom business

Cloud compliance myths — **busted**

Misunderstandings around cloud compliance can quietly erode your legal defences. Let's set the record straight.

"Our provider says they're compliant, so we're fine."	If a breach happens, the Information Regulator knocks on your door, not your cloud provider's.
"Data stored in the cloud is always encrypted."	Often false. Encryption is not automatically applied across all cloud tiers.
"Offshore storage isn't a problem if you're using a big name."	Some of the largest cloud providers default to overseas storage. Without explicit consent and equivalent protections, that's a direct POPIA violation.
"We've never had a breach, so our setup must be secure."	That's like saying you don't need a fire extinguisher because your office hasn't burned down yet.
"POPIA only applies to personal information, and we don't handle much of that."	If you collect names, emails, employee records, or client invoices — welcome to the definition of personal information.

vodacom business

Real stories. **Real** consequences.

When cloud compliance fails, the fallout can be severe — but these are avoidable lessons.

University insider threat at Tshwane University of Technology

A 2024 study revealed that inadequate insider training and weak policy enforcement led to cloud data leakage in a major South African university, where employees inadvertently exposed sensitive information in shared cloud environments.

Lesson: Human risk in cloud setups is real — robust access controls, training, and monitoring are essential.

Financial services sector — cloud compliance roadmap matter

AVeS Cyber Security collaborated with a South African financial organisation to build a cloud migration plan. They discovered that assumptions around cloud-native security led to hidden vulnerabilities. The firm redesigned access governance, layered in encryption, SIEM, and multi-factor authentication to align with POPIA.

Lesson: Cloud security needs purposeful design; "lift-and-shift" is often insufficient under POPIA.

For most businesses, cloud compliance is about **building trust, protecting customer relationships, and unlocking real digital transformation.**

More than that, it's about future-proofing. As regulations evolve and digital ecosystems expand, businesses that treat compliance as an ongoing strategy — not a once-off policy — will be the ones that lead. They'll be able to adapt faster, respond confidently to audits, and scale without fear of legal disruption.

It's all about **partnering smart, acting proactively,** and **keeping compliance embedded** in every cloud decision you make.

vodacom business


vodacom
business